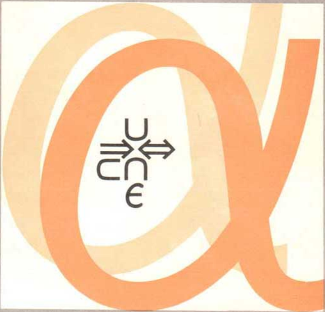
# ALGEBRA I

ARMANDO O. ROJO



EDITORIAL "EL ATENEO" BUENOS AIRES

LIBROS
NORAY
ESTADO 319
Teléfono 31728
Santiago

# álgebra I

*Del mismo autor*

ALGEBRA II

Espacios vectoriales. Matrices.
Trasformaciones lineales.
Diagonalización.

# álgebra I

**Armando O. Rojo**

8ª edición

LIBRERIA **'EL ATENEO'** EDITORIAL

BUENOS AIRES - LIMA - RIO DE JANEIRO - CARACAS - MEXICO - BARCELONA - MADRID - BOGOTA

Todos los derechos reservados.
Este libro no puede reproducirse, total o parcialmente,
por ningún método gráfico, electrónico o mecánico,
incluyendo los sistemas de fotocopia, registro magnetofónico
o de alimentación de datos, sin expreso consentimiento del editor.

Queda hecho el depósito que previene la ley N° 11.723
© 1972, 1974, 1975 (3a. y 4a. ed.), 1976, 1978 (6a. y 7a. ed.). 1981
"El Ateneo" Pedro García S.A.
Librería, Editorial e Inmobiliaria, Florida 340, Buenos Aires
Fundada en 1912 por don Pedro García.

IMPRESO EN LA ARGENTINA

## PROLOGO

*La enseñanza de los contenidos fundamentales del álgebra actual y el uso de su peculiar terminología son una realidad en todos los cursos básicos a nivel universitario y profesoral. Creo que hay dos razones principales que dan crédito a esa determinación: una asociada al progreso de las ciencias, a la unidad conceptual y, en última instancia, al mundo de la inteligencia; la otra vinculada estrechamente a sus aplicaciones en casi todas las disciplinas de interés práctico y de vigencia cotidiana.*

*No escapan a estas consideraciones las dificultades que se presentan inicialmente ante lo que es, de alguna manera, nuevo. Precisamente esa constancia me ha movido a redactar este texto elemental de álgebra, en el que he procurado desarrollar sus contenidos con una metodología que estimo apropiada. Se han intercalado ejemplos que, además de ilustrar la teoría, hacen posible la adquisición de métodos adecuados de trabajo. Un detalle que juzgo de interés para los lectores es la respuesta que se da a los problemas propuestos, o al menos la sugerencia de pautas para las demostraciones que figuran en los trabajos prácticos.*

*Doy testimonio de mi agradecimiento a los amigos que me han ayudado y estimulado en esta tarea, y a la Editorial EL ATENEO, cuyo personal no ha escatimado esfuerzos para resolver las dificultades inherentes a la publicación del texto.*

ARMANDO O. ROJO

## CONTENIDO


**Capítulo 1. NOCIONES DE LOGICA** 1

1. 2. Proposiciones 1
1. 3. Notaciones y conectivos 2
1. 4. Operaciones proposicionales 2
1. 5. Condiciones necesarias y suficientes 7
1. 6. Leyes lógicas 8
1. 7. Implicaciones asociadas 11
1. 8. Negación de una implicación 12
1. 9. Razonamiento deductivo válido 13
1.10. Funciones proposicionales 14
1.11. Circuitos lógicos 18
Trabajo Práctico I 22

**Capítulo 2. CONJUNTOS** 25

2. 2. Determinación de conjuntos 25
2. 3. Inclusión 30
2. 4. Conjunto de partes 34
2. 5. Complementación 36
2. 6. Intersección 38
2. 7. Unión 42
2. 8. Leyes distributivas 45
2. 9. Leyes de De Morgan 46
2.10. Diferencia 48
2.11. Diferencia simétrica 50
2.12. Producto cartesiano 53
2.13. Operaciones generalizadas 56
2.14. Uniones disjuntas 58
Trabajo Práctico II 60

**Capítulo 3. RELACIONES** 64

3. 2. Relaciones binarias 64
3. 3. Representación de relaciones 65

3. 4. Dominio, imagen, relación inversa 66
3. 5. Composición de relaciones 68
3. 6. Relaciones en un conjunto 69
3. 7. Propiedades de las relaciones 71
3. 8. Relaciones de equivalencia 77
3. 9. Relaciones de orden 90
Trabajo Práctico III 98

Capítulo 4. FUNCIONES 102
4. 2. Relaciones funcionales 102
4. 3. Representación de funciones 105
4. 4. Clasificación de funciones 110
4. 5. Funciones especiales 114
4. 6. Composición de funciones 117
4. 7. Funciones inversas 121
4. 8. Imágenes de subconjuntos del dominio 128
4. 9. Preimágenes de partes del codominio 131
4.10. Restricción y extensión de una función 137
Trabajo Práctico IV 138

Capítulo 5. LEYES DE COMPOSICION 142
5. 2. Leyes de composición interna 142
5. 3. Propiedades y elementos distinguidos 144
5. 4. Homomorfismos 151
5. 5. Compatibilidad de una relación de equivalencia con una ley interna 154
5. 6. Ley de composición externa 158
Trabajo Práctico V 160

Capítulo 6. COORDINABILIDAD. INDUCCION COMPLETA. COMBINATORIA 162
6. 2. Conjuntos coordinables o equipotentes 162
6. 3. Conjuntos finitos y numerables 164
6. 4. Inducción completa 167
6. 5. El símbolo de sumatoria 170
6. 6. La función factorial 176
6. 7. Números combinatorios 177
6. 8. Potencia de un binomio 179
6. 9. Funciones entre intervalos naturales 186
6.10. Combinatoria simple y con repetición 197
Trabajo Práctico VI 204

CONTENIDO


Capítulo 7. SISTEMAS AXIOMATICOS 208

7. 2. Sistemas axiomáticos 208
7. 3. Algebra de Boole 210
7. 4. Sistema axiomático de Peano 212
7. 5. Estructura de monoide 219
7. 6. Estructura de semigrupo 220
Trabajo Práctico VII 223

Capítulo 8. ESTRUCTURA DE GRUPO 225

8. 2. El concepto de grupo 225
8. 3. Propiedades de los grupos 228
8. 4. Subgrupos 231
8. 5. Operaciones con subgrupos 235
8. 6. Homomorfismos de grupos 237
8. 7. Núcleo e imagen de un morfismo de grupos 240
8. 8. Relación de equivalencia compatible 247
8. 9. Subgrupos distinguidos 248
8.10. Subgrupos normales o invariantes 252
8.11. Grupo cociente asociado a un subgrupo 254
8.12. Grupos cíclicos 257
8.13. Traslaciones de un grupo 258
8.14. Grupos finitos 259
Trabajo Práctico VIII 261

Capítulo 9. ESTRUCTURAS DE ANILLO Y DE CUERPO. ENTEROS Y RACIONALES 264

9. 2. Estructura de anillo 264
9. 3. Propiedades de los anillos 266
9. 4. Anillo sin divisores de cero 267
9. 5. Dominio de integridad 272
9. 6. Subanillos e ideales 272
9. 7. Factorización en un anillo 274
9. 8. Anillo ordenado 276
9. 9. Estructura de cuerpo 278
9.10. Dominio de integridad de los enteros 280
9.11. Isomorfismo de los enteros positivos con N 284
9.12. Propiedades del valor absoluto 285
9.13. Algoritmo de la división entera 287
9.14. Algoritmo de Euclides 288
9.15. Números primos 290
9.16. El cuerpo de los racionales 293

9.17. Isomorfismo de una parte de **Q** en **Z** 298
9.18. Relación de orden en **Q** 301
9.19. Numerabilidad de **Q** 301
Trabajo Práctico IX 303

**Capítulo 10. NUMEROS REALES** 308

10. 2. El número real 308
10. 3. Operaciones en **R** 315
10. 4. Isomorfismo de una parte de **R** en **Q** 321
10. 5. Cuerpo ordenado y completo de los reales 321
10. 6. Cortaduras en **Q** 321
10. 7. Completitud de **R** 326
10. 8. Potenciación en **R** 329
10. 9. Logaritmación en $\mathbf{R}^+$ 333
10.10. Potencia del conjunto **R** 335
Trabajo Práctico X 338

**Capítulo 11. EL CUERPO DE LOS NUMEROS COMPLEJOS** 341

11. 2. El número complejo 341
11. 3. Isomorfismo de los complejos reales en los reales 347
11. 4. Forma binómica de un complejo 347
11. 5. La conjugación en **C** 349
11. 6. Módulo de un complejo 351
11. 7. Raíz cuadrada en **C** 354
11. 8. Forma polar o trigonométrica 356
11. 9. Operaciones en forma polar 358
11.10. Radicación en **C** 362
11.11. Forma exponencial en **C** 366
11.12. Logaritmación en **C** 367
11.13. Exponencial compleja general 369
11.14. Raíces primitivas de la unidad 370
Trabajo Práctico XI 373

**Capítulo 12. POLINOMIOS** 378

12. 2. Anillo de polinomios formales de un anillo 378
12. 3. Anillo de polinomios de un cuerpo 383
12. 4. Divisibilidad en el dominio **K** [X] 384
12. 5. Ideales de **K** [X] 388
12. 6. Factorización en **K** [X] 389
12. 7. Especialización de X y raíces de polinomios 396

12. 8. Raíces múltiples 399
12. 9. Polinomio derivado y raíces múltiples 400
12.10. Número de raíces de polinomios 401
12.11. Raíces de polinomios reales 403
12.12. Relaciones entre raíces y coeficientes 407
12.13. Fórmula de Taylor y Método de Horner 409
Trabajo Práctico XII 414

**BIBLIOGRAFIA** 417

**RESPUESTAS A LOS TRABAJOS PRACTICOS** 419

**INDICE** 473

## Capítulo 1

# NOCIONES DE LOGICA

### 1.1. INTRODUCCION

Todo desarrollo matemático exige razonar en forma válida acerca de cosas trascendentes y particularmente abstractas. Hay que comenzar por eliminar las ambigüedades del lenguaje ordinario, introduciendo símbolos y conectivos cuyo uso adecuado descarte las contingencias, aporte claridad y economía de pensamiento. En este capítulo introducimos el concepto de proposición, las operaciones proposicionales y sus leyes, reglas de inferencia, y la cuantificación de funciones proposicionales, cuyo uso estará presente en todo el texto.

### 1.2. PROPOSICIONES

Consideramos las siguientes oraciones:

1. ¿Quién viene?
2. Deténgase
3. El calor dilata los cuerpos
4. 4 es un número impar
5. Juan ama la música
6. La música es amada por Juan

Se trata de seis oraciones diferentes, una interrogativa, una orden y cuatro declarativas. De las dos primeras no podemos decir que sean verdaderas ni falsas; una pregunta puede formularse o nó, y una orden puede ser cumplida o no. En cambio, de las cuatro últimas, que son declarativas, tiene sentido decir si son verdaderas o falsas. A éstas las llamamos proposiciones.

***Definición***

Proposición es toda oración respecto de la cual puede decirse si es verdadera falsa.

Es decir, proposición es toda oración declarativa. Toda proposición está asociada a un valor de verdad, el cual puede ser verdadero (V) o bien falso (F). Las oraciones (5) y (6) son diferentes desde el punto de vista gramatical; el objeto directo de la (5) es el sujeto de la (6), pero ambas tienen el mismo significado, y las consideramos como la misma proposición. Podemos decir entonces *proposición es el significado de toda oración declarativa.*

## 1.3. NOTACIONES Y CONECTIVOS

Las proposiciones genéricas son denotadas con las letras $p$, $q$, $r$, etc. A partir de proposiciones simples es posible generar otras, simples o compuestas. Es decir, se puede operar con proposiciones, y según sean tales operaciones se utilizan ciertos símbolos, llamados conectivos lógicos.

| Conectivo | Operación asociada | Significado |
|---|---|---|
| $\sim$ | Negación | no $p$ o no es cierto que $p$ |
| $\wedge$ | Conjunción o producto lógico | $p$ y $q$ |
| $\vee$ | Disyunción o suma lógica | $p$ o $q$ (en sentido incluyente) |
| $\Rightarrow$ | Implicación | $p$ implica $q$ o si $p$, entonces $q$ |
| $\Leftrightarrow$ | Doble implicación | $p$ si y sólo si $q$ |
| $\veebar$ | Diferencia simétrica | $p$ o $q$ (en sentido excluyente) |

## 1.4. OPERACIONES PROPOSICIONALES

Definiremos las operaciones entre proposiciones en el sentido siguiente: dadas una o dos proposiciones, cuyos valores de verdad se conocen, se trata de caracterizar la proposición resultante a través de su valor de verdad. Se supone que en la elección de estos valores se tiene en cuenta el buen sentido.

### 1.4.1. Negación

*Definición*

Negación de la proposición $p$ es la proposición $\sim p$ (no $p$), cuya tabla de valores de verdad es

| $p$ | $\sim p$ |
|---|---|
| V | F |
| F | V |

Se trata de una operación unitaria, pues a partir de una proposición se obtiene otra, que es su negación.

*Ejemplo 1-1.*

La negación de

$p$ : todo hombre es honesto

es $\sim p$ : no todo hombre es honesto

o bien: $\sim p$ : no es cierto que todo hombre es honesto

$\sim p$ : hay hombres que no son honestos

$\sim p$ : existen hombres deshonestos

la cual es V, ya que la primera es F.

### 1.4.2. Conjunción

*Definición*

Conjunción de las proposiciones $p$ y $q$ es la proposición $p \wedge q$ ($p$ y $q$), cuya tabla de valores de verdad es

| $p$ | $q$ | $p \wedge q$ |
|---|---|---|
| V | V | V |
| V | F | F |
| F | V | F |
| F | F | F |

La tabla que define la operación establece que la conjunción sólo es verdadera si lo son las dos proposiciones componentes. En todo otro caso es falsa.

*Ejemplo 1-2.*

Si declaramos

i) 3 es un número impar y 2 es un número primo

se trata de la conjunción de las proposiciones

$p$ : 3 es un número impar

$q$ : 2 es un número primo

y por ser ambas verdaderas, la proposición compuesta es V.

ii) hoy es lunes y mañana es jueves

esta conjunción es F, ya que no coexisten las verdades de $p$ y $q$.

### 1.4.3. Disyunción

*Definición*

Disyunción de las proposiciones $p$ y $q$ es la proposición $p \vee q$ ($p$ o $q$) cuya tabla de valores de verdad es

| $p$ | $q$ | $p \vee q$ |
|---|---|---|
| V | V | V |
| V | F | V |
| F | V | V |
| F | F | F |

La conjunción *o* es utilizada en sentido incluyente, ya que la verdad de la disyunción se da en el caso de que al menos una de las proposiciones sea V. En el lenguaje ordinario la palabra *o* es utilizada en sentido excluyente o incluyente.

La ambigüedad se elimina con la elección del símbolo adecuado.

En matemática se utiliza la disyunción definida por la tabla precedente, la cual agota toda posibilidad.

La disyunción sólo es F en el caso en que las dos proposiciones componentes sean falsas.

***Ejemplo 1-3.***

i ) hoy es lunes o martes

representa la disyunción de las proposiciones $p$: hoy es lunes y $q$: hoy es martes. El sentido de la conjunción *o* es exlcuyente, ya que $p$ y $q$ no pueden ser simultáneamente verdaderas. No obstante, la proposición compuesta puede analizarse a la luz de la tabla propuesta, a través de los tres últimos renglones, y será falsa sólo si las dos lo son.

ii ) regalo los libros viejos o que no me sirven

es la disyunción de las proposiciones

$p$ : regalo los libros viejos
$q$ : regalo los libros que no me sirven

El sentido del *o* es incluyente, pues si en efecto regalo un libro que es viejo, y que además no me sirve, entonces $p \vee q$ es V.

iii) 3 es un número impar o 4 es un número primo

es una propoposición V, pues la primera es V.

### 1.4.4. Implicación o Condicional

***Definición***

Implicación de las proposiciones $p$ y $q$ es la proposición $p \Rightarrow q$ ($p$ implica $q$, si $p$ entonces $q$) cuya tabla de valores de verdad es

| $p$ | $q$ | $p \Rightarrow q$ |
|---|---|---|
| V | V | V |
| V | F | F |
| F | V | V |
| F | F | V |

Las proposiciones $p$ y $q$ se llaman antecedente y consecuente de la implicación o condicional. La implicación usual en matemática es formal en el sentido de que no es necesario que el consecuente se derive lógicamente del antecedente; cuando esto ocurre, la implicación se llama material y queda incluida en la primera.

Las tablas de valores de verdad se definen arbitrariamente, pero respetando el sentido común. Enunciamos la siguiente proposición:

"SI apruebo el examen, ENTONCES te presto el apunte" (1)

Se trata de la implicación de las proposiciones

$p$ : apruebo el examen
$q$ : te presto el apunte

Interesa inducir la verdad o falsedad de la implicación (1), en términos de la V o F de las proposiciones $p$ y $q$. El enunciado (1) puede pensarse como un compromiso, condicionado por $p$, y podemos asociar su verdad al cumplimiento del compromiso. Es obvio que si $p$ es F, es decir, si no apruebo el examen, quedo liberado del compromiso, y preste o no preste el apunte la proposición (1) es V. Es decir, si el antecedente es F, la implicación es V

Si $p$ es V, en cuyo caso apruebo el examen, y no presto el apunte, el compromiso no se cumple, y la proposición (1) es entonces F. Si $p$ y $q$ son V, entonces la implicación es V porque el compromiso se cumple.

De este modo, la implicación sólo es falsa cuando el antecedente es V y el consecuente es F.

***Ejemplo 1-4.***

i) si hoy es lunes, entonces mañana es martes

es la implicación de las proposiciones

$p$ : hoy es lunes
$q$ : mañana es martes

Como no puede darse antecedente V y consecuente F, la implicación es V.

ii) $1 = -1 \Rightarrow 1^2 = (-1)^2$

es V por ser el antecedente F.

### 1.4.5. Doble implicación o bicondicional

***Definición***

Doble implicación de las proposiciones $p$ y $q$ es la proposición $p \Leftrightarrow q$ ($p$ si y sólo si $q$), cuya tabla de valores de verdad es

| $p$ | $q$ | $p \Leftrightarrow q$ |
|---|---|---|
| V | V | V |
| V | F | F |
| F | V | F |
| F | F | V |

La doble implicación o bicondicional sólo es verdadera si ambas proposiciones tienen el mismo valor de verdad.

La doble implicación puede definirse como la conjunción de una implicación y su recíproca. De este modo, la tabla de valores de verdad de $p \Leftrightarrow q$, puede obtenerse mediante la tabla de $(p \Rightarrow q) \wedge (q \Rightarrow p)$, como sigue

| $p$ | $q$ | $p \Rightarrow q$ | $q \Rightarrow p$ | $(p \Rightarrow q) \wedge (q \Rightarrow p)$ |
|---|---|---|---|---|
| V | V | V | V | V |
| V | F | F | V | F |
| F | V | V | F | F |
| F | F | V | V | V |

***Ejemplo 1-5.***

i) T es equilátero si y sólo si T es equiángulo

es la doble implicación de las proposiciones

$p$ : T es equilátero
$q$ : T es equiángulo

Toda vez que $p$ sea V, también lo es $q$, y análogamente, si $p$ es F, $q$ es F. De modo que la doble implicación es V.

ii) $a = b$ si y sólo si $a^2 = b^2$

las proposiciones son

$$p : a = b$$
$$q : a^2 = b^2$$

la doble implicación propuesta es falsa si $p$ es F y $q$ es V. En los demás casos es V.

### 1.4.6. Diferencia simétrica

***Definición***

Diferencia simétrica o disyunción excluyente de las proposiciones $p$ y $q$ es la proposición $p \veebar q$ ($p$ o $q$, en sentido excluyente) cuya tabla de valores de verdad es

| $p$ | $q$ | $p \veebar q$ |
|---|---|---|
| V | V | F |
| V | F | V |
| F | V | V |
| F | F | F |

La verdad de $p \veebar q$ está caracterizada por la verdad de una y sólo una de las proposiciones componentes.

Es claro que $p \veebar q$ equivale a la negación de $p \Leftrightarrow q$.

## 1.5. CONDICIONES NECESARIAS Y SUFICIENTES

Consideramos la tabla de valores de verdad de la implicación

| $p$ | $q$ | $p \Rightarrow q$ |
|---|---|---|
| V | V | V |
| V | F | F |
| F | V | V |
| F | F | V |

Hay tres casos en que $p \Rightarrow q$ es V, y entre ellos hay uno en que $p$ es V, en el cual resulta $q$ verdadera. Es obvio que nos referimos al primer renglón de la tabla, y se tiene que si $p \Rightarrow q$ es V y $p$ es V, entonces $q$ es V. Se dice entonces que el antecedente $p$ es condición suficiente para el consecuente $q$.

En cambio, si $p$ es F, nada podemos decir de $q$, puesto que puede ser V o F. Por otra parte, cuando $p \Rightarrow q$ es V, si $q$ es V, entonces $p$ puede ser V o F; mas para que $p$ sea V se necesita que $q$ lo sea. Se dice entonces que $q$ es condición necesaria para $p$.

Resumiendo, si $p \Rightarrow q$ es V, entonces $p$ es condición suficiente para $q$ y $q$ es condición necesaria para $p$.

Estas condiciones suelen expresarse así:

$q$ si $p$ (condición suficiente)
$p$ sólo si $q$ (condición necesaria)

***Ejemplo 1-6.***

La siguiente implicación es V:

"SI T es equilátero, ENTONCES T es isósceles"

En este caso $p$ : T es equilátero
$q$ : T es isósceles

y $p$ es condición suficiente para $q$, es decir, que un triángulo sea equilátero es suficiente para asegurar que sea isósceles. Por otra parte, T es equilátero sólo si es isósceles; es decir, que un triángulo sea isósceles es necesario para que sea equilátero.

Sea ahora la doble implicación $p \Leftrightarrow q$, es decir $(p \Rightarrow q) \wedge (q \Rightarrow p)$. Si $p \Leftrightarrow q$ es V, entonces $p \Rightarrow q$ es V y $q \Rightarrow p$ es V. Se tiene, atendiendo a la primera, que $p$ es condición suficiente para $q$; y, teniendo en cuenta la segunda implicación, ocurre que $p$ es condición necesaria para $q$.

Es decir, si $p \Leftrightarrow q$ es V, entonces el antecedente $p$ es condición necesaria y suficiente para el consecuente $q$.

Análogamente, en el caso de doble implicación verdadera, el consecuente $q$ es también condición necesaria y suficiente para el antecedente $p$.

***Ejemplo 1-7.***

La proposición

"T es equilátero SI Y SOLO SI T es equiángulo"

es la doble implicación de las proposiciones

$p$ : T es equilátero
$q$ : T es equiángulo

Aquélla es V, y cualquiera de las dos proposiciones es condición necesaria y suficiente para la otra.

## 1.6. LEYES LOGICAS

Consideremos la proposición

$$[(p \Rightarrow q) \wedge p] \Rightarrow q \qquad (1)$$

cuya tabla de valores de verdad es:

| $p$ | $q$ | $p \Rightarrow q$ | $(p \Rightarrow q) \wedge p$ | $[(p \Rightarrow q) \wedge p] \Rightarrow q$ |
|---|---|---|---|---|
| V | V | V | V | V |
| V | F | F | F | V |
| F | V | V | F | V |
| F | F | V | F | V |

La proposición compuesta (1) es V, independientemente de los valores de verdad de las proposiciones componentes. Se dice entonces que tal proposición es una tautología o ley lógica.

La proposición $p \Rightarrow p$ es V cualquiera que sea el valor de verdad de $p$. Es otro ejemplo de una ley lógica.

En cambio $p \wedge \sim p$ es F, cualquiera que sea $p$. Se dice que es una contradicción.

En el cálculo proposicional se utilizan las siguientes leyes o tautologías cuya demostración se reduce a la confección de la correspondiente tabla de valores de verdad:

### 1.6.1. Involución

$$\sim(\sim p) \Leftrightarrow p$$

el modo de leerla es: "no, no $p$, equivale a $p$".

### 1.6.2. Idempotencia

$$(p \wedge p) \Leftrightarrow p$$
$$(p \vee p) \Leftrightarrow p$$

### 1.6.3. Conmutatividad

a) de la disyunción $\quad p \vee q \Leftrightarrow q \vee p$

b) de la conjunción $\quad p \wedge q \Leftrightarrow q \wedge p$

### 1.6.4. Asociatividad

a) de la disyunción

$$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$$

b) De la conjunción

$$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$$

### 1.6.5. Distributividad

a) de la conjunción respecto de la disyunción

$$(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$$

b) de la disyunción respecto de la conjunción

$$(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$$

### 1.6.6. Leyes de De Morgan

a) La negación de una disyunción es equivalente a la conjunción de las negaciones

$$\sim (p \vee q) \Leftrightarrow \sim p \wedge \sim q$$

b) La negación de una conjunción es equivalente a la disyunción de las negaciones

$$\sim (p \wedge q) \Leftrightarrow \sim p \vee \sim q$$

***Ejemplo 1-8.***

Tabla de valores de verdad de la distributividad de la conjunción respecto de la disyunción:

$$(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$$

Cada valor de verdad de $p$ puede asociarse a dos valores de verdad de $q$, y por cada uno de estos pares de valores se tienen dos posibilidades para $r$; en consecuencia, resultan $2^3 = 8$ renglones en la tabla. Si se dan $n$ proposiciones, en la tabla hay que analizar $2^n$ renglones.

Por otra parte, es posible simplificar la confección de la tabla, como se indica a continuación

| $(p$ | $\vee$ | $q)$ | $\wedge$ | $r$ | $\Leftrightarrow$ | $(p \wedge r)$ | $\vee$ | $(q \wedge r)$ |
|---|---|---|---|---|---|---|---|---|
| V | V | V | V | V | V | V | V | V |
| V | V | V | F | F | V | F | F | F |
| V | V | F | V | V | V | V | V | F |
| V | V | F | F | F | V | F | F | F |
| F | V | V | V | V | V | V | V | V |
| F | V | V | F | F | V | F | F | F |
| F | F | F | F | V | V | F | F | F |
| F | F | F | F | F | V | F | F | F |

***Ejemplo 1-9.***

Confeccionamos la tabla de valores de verdad de la siguiente ley de **De Morgan**:

$$\sim (p \wedge q) \Leftrightarrow \sim p \vee \sim q$$

| $\sim$ | $(p$ | $\wedge$ | $q)$ | $\Leftrightarrow$ | $\sim p$ | $\vee$ | $\sim q$ |
|---|---|---|---|---|---|---|---|
| F | V | V | V | V | F | F | F |
| V | V | F | F | V | F | V | V |
| V | F | F | V | V | V | V | F |
| V | F | F | F | V | V | V | V |

***Ejemplo 1-10.***

La proposición

$$(p \wedge q) \Rightarrow p$$

es una ley lógica, pues la tabla

| $(p$ | $\wedge$ | $q)$ | $\Rightarrow$ | $p$ |
|---|---|---|---|---|
| V | V | V | V | V |
| V | F | F | V | V |
| F | F | V | V | F |
| F | F | F | V | F |

nos muestra que es una tautología.

## 1.7. IMPLICACIONES ASOCIADAS

Sea el condicional $p \Rightarrow q$, que llamamos directo; en conexión con él, se presentan otros tres, obtenidos por permutaciones o negaciones del antecedente y consecuente:

$q \Rightarrow p$ recíproco
$\sim p \Rightarrow \sim q$ contrario
$\sim q \Rightarrow \sim p$ contrarrecíproco

Las cuatro implicaciones propuestas se llaman conjugadas, y cualquiera de ellas puede tomarse como directa. El siguiente esquema nos proporciona la relación que las vincula:

Es fácil verificar que las implicaciones contrarrecíprocas son equivalentes, es decir, los siguientes bicondicionales son tautologías:

$$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$$

$$(q \Rightarrow p) \Leftrightarrow (\sim p \Rightarrow \sim q)$$

Si la implicación directa es V, también lo es la contrarrecíproca, y no podemos afirmar la verdad de la recíproca o de la contraria. Pero si son verdaderos un

condicional y su recíproco o contrario, entonces son verdaderos los cuatro, y las proposiciones antecedente y consecuente son equivalentes.

Se presenta continuamente la necesidad de demostrar la verdad de $p \Rightarrow q$, y de acuerdo con lo expuesto se presentan dos métodos:

i) *directo.* Si $p$ es F, nada hay que probar, pues en este caso $p \Rightarrow q$ es V. Si $p$ es V hay que establecer que el valor de verdad de $q$ es V.

ii) *indirecto.* Si $q$ es V queda establecida la verdad de $p \Rightarrow q$. Pero si $q$ es F hay que examinar $p$ y llegar a establecer que su valor de verdad es F.

## 1.8. NEGACION DE UNA IMPLICACION

Las proposiciones $p \Rightarrow q$ y $\sim(p \wedge \sim q)$ son equivalentes, como lo muestra la siguiente tabla

| $(p$ | $\Rightarrow$ | $q)$ | $\Leftrightarrow$ | $\sim$ | $(p \wedge \sim q)$ |
|---|---|---|---|---|---|
| V | V | V | V | V | V F F |
| V | F | F | V | F | V V V |
| F | V | V | V | V | F F F |
| F | V | F | V | V | F F V |

En consecuencia, la negación de la primera equivale a la negación de la segunda, es decir

$$\sim(p \Rightarrow q) \Leftrightarrow \sim[\sim(p \wedge \sim q)]$$

y por 1.6.1, se tiene

$$\sim(p \Rightarrow q) \Leftrightarrow (p \wedge \sim q)$$

Es decir, la negación de una implicación no es una implicación, sino la conjunción del antecedente con la negación del consecuente.

***Ejemplo 1-11.***

Sean las implicaciones

i) Si hoy es lunes, entonces mañana es miércoles.

ii) $1 = -1 \Rightarrow 1^2 = (-1)^2$

Sus negaciones son, respectivamente,

"Hoy es lunes y mañana no es miércoles"

" $1 = -1 \wedge 1^2 \neq (-1)^2$ "

## 1.9. RAZONAMIENTO DEDUCTIVO VALIDO

En matemática interesa el tipo de razonamiento llamado deductivo. Llamamos razonamiento a un par ordenado $(\{p_i\}; q)$, siendo $\{p_i\}$ un conjunto finito de proposiciones, llamadas premisas, y $q$ una proposición, llamada conclusión, respecto de la cual se afirma que deriva de las premisas.

Un razonamiento es deductivo si y sólo si las premisas son evidencias de la verdad de la conclusión, es decir, si $p_1, p_2, \ldots, p_n$ son verdaderas, entonces $q$ verdadera. Un razonamiento deductivo es válido si no es posible que las premisas sean verdaderas y la conclusión falsa. De un razonamiento no se dice que es V o F, sino que es válido o no.

Llamamos regla de inferencia, a todo esquema válido de razonamiento, independientemente de la V o F de las proposiciones componentes. De este modo, toda regla de inferencia es tautológica.

Un razonamiento deductivo es válido cuando el condicional cuyo antecedente es la conjunción de las premisas, y el consecuente es la conclusión, es tautológico.

Son ejemplos de reglas de inferencia:

a) Ley del *modus ponens:*

$$\text{SI } p \text{ y } p \Rightarrow q, \text{ ENTONCES } q$$

La notación clásica es

$$\begin{array}{c} p \\ p \Rightarrow q \\ \hline q \end{array}$$

b) Ley del *modus tolens:*

$$\begin{array}{c} p \Rightarrow q \\ \sim q \\ \hline \sim p \end{array}$$

Este esquema es la notación clásica del condicional

$$[(p \Rightarrow q) \ \wedge \ \sim q] \Rightarrow \sim p$$

c) Ley del silogismo hipotético:

$$\begin{array}{c} p \Rightarrow q \\ q \Rightarrow r \\ \hline p \Rightarrow r \end{array}$$

Es decir, la proposición $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$ es una tautología.

En cambio, el condicional $[(p \Rightarrow q) \wedge q] \Rightarrow p$ no es una forma válida de

razonamiento, ya que la correspondiente tabla de valores de verdad nos muestra que no es tautológico.

*Ejemplo 1-12.*

*a)* Justificar la validez del razonamiento

$$\begin{array}{c} p \Rightarrow q \\ \sim r \Rightarrow \sim q \\ \sim(\sim p \ \wedge \ \sim t) \\ t \Rightarrow s \\ \sim r \\ \hline s \end{array}$$

En lugar de confeccionar la tabla del condicional entre la conjunción de las premisas y la conclusión, haremos uso de las leyes del cálculo proposicional, a fin de simplificar la situación. La segunda premisa es equivalente a la contrarrecíproca $q \Rightarrow r$; por la ley del silogismo hipotético, de la primera y de ésta, resulta $p \Rightarrow r$. La última premisa es V, y en consecuencia $r$ es F, y como $p \Rightarrow r$ es V resulta necesariamente que $p$ es F. La tercera premisa equivale a $p \vee t$, de acuerdo con una ley de De Morgan, y por ser $p$ falsa resulta la verdad de $t$. Ahora bien, siendo $t$ y $t \Rightarrow s$ verdaderos, resulta la verdad de $s$, por 1.9 a).

*b)* Justificar la validez del razonamiento cuyas premisas son:

Hoy llueve o hace frío,
Hoy llueve o no hace frío,

y la conclusión: Hoy llueve.
En lenguaje simbólico se tiene

$$\begin{array}{c} p \vee q \\ p \vee \sim q \\ \hline p \end{array}$$

$q$, o bien $\sim q$ es F; cualquiera que sea el caso, por ser las disyunciones verdaderas, resulta que $p$ es V. De otro modo, la conjunción de ambas disyunciones, por la distributividad, es equivalente a $p \vee (q \wedge \sim q)$. La verdad de aquéllas asegura la verdad de ésta, y como $q \wedge \sim q$ es F, resulta la verdad de $p$.

## 1.10. FUNCIONES PROPOSICIONALES. SU CUANTIFICACION

El símbolo P $(x)$ es la representación de un predicado o propiedad relativos al objeto indeterminado $x$, perteneciente a cierto universo o conjunto. Si nos referimos a

los números enteros y estamos interesados en la propiedad de ser impar, entonces la traducción de P $(x)$ consiste en: $x$ es impar, y se escribe

$$P(x) : x \text{ es impar}$$

Es claro que el enunciado: "$x$ es impar" no es una proposición, ya que a menos que se especifique a $x$ no podemos decir nada acerca de su verdad o falsedad. Ocurre, sin embargo, que para cada asignación dada al sujeto $x$ dicho enunciado es una proposición. A expresiones de este tipo se las llama funciones o esquemas proposicionales.

***Definición***

Función proposicional en una variable o indeterminada $x$ es toda oración en la que figura $x$ como sujeto u objeto directo, la cual se convierte en proposición para cada especificación de $x$.

En nuestro ejemplo resultan proposiciones como

$P(-4) : -4$ es impar (F)
$P(\ 5) :\ 5$ es impar (V), etc.

Se presentan también funciones proposicionales con dos variables o indeterminadas. Sea, por ejemplo

$$P(x\ ,y) : x \text{ es divisor de } y$$

Lo mismo que en el caso anterior, si $x$ e $y$ son enteros, P $(x\ ,y)$ no es proposición, ya que no podemos afirmar la verdad o falsedad del enunciado. Mas para cada particularización de valores se tiene una proposición

$P(-2, 6) : -2$ es divisor de 6 (V)
$P(\ 12, 6) :\ 12$ es divisor de 6 (F)

A partir de funciones proposicionales es posible obtener proposiciones generales mediante un proceso llamado de cuantificación. Asociados a la indeterminada $x$, introducimos los símbolos $\forall x$ y $\exists x$, llamados cuantificadores universal y existencial en $x$, respectivamente. Las expresiones

Para todo $x$, se verifica P $(x)$
Existe $x$, tal que se verifica P $(x)$

se denotan mediante $\forall x :\ P(x)$ (1)
$\exists x /\ P(x)$ (2)

y corresponden a una función proposicional P $(x)$ cuantificada universalmente en el primer caso, y existencialmente en el segundo. Una función proposicional cuantificada

adquiere el carácter de proposición. En efecto, retomando el primer ejemplo, si decimos

"Todos los números enteros son impares". (1')

es claro que hemos enunciado una proposición general y relativa a todos los números enteros, cuyo valor de verdad es F. Una traducción más detallada de esta proposición consiste en

"Cualquiera que sea $x$, $x$ es impar".

Es decir $\forall x : x$ es impar

Si cuantificamos existencialmente la misma función proposicional, se tiene

$\exists x / x$ es impar

O sea "Existe $x$, tal que $x$ es impar".

O bien "Existen enteros que son impares". (2')

O más brevemente "Hay enteros impares".

El valor de verdad es V, y en consecuencia se trata de una proposición. El cuantificador existencial se refiere a, por lo menos, un $x$.

Es obvio que una función proposicional cuantificada universalmente es V si y sólo si son V todas las proposiciones particulares asociadas a aquélla. Para asegurar la verdad de una función proposioional, cuantificada existencialmente, es suficiente que sea verdadera alguna de las proposiciones asociadas a la función proposicional.

Un problema de interés es la negación de funciones proposicionales cuantificadas. La negación (1') es

"No todos los enteros son impares"

es decir "Existen enteros que no son impares"

y en símbolos $\exists x / \sim P(x)$

Entonces, para negar una función proposicional cuantificada **universalmente** se cambia el cuantificador en existencial, y se niega la función **proposicional.**

La negación de (2') es

"No existen enteros impares".

Es decir "Cualquiera que sea el entero, no es impar"

o lo que es lo mismo

"Todo entero es par".

En símbolos $\forall x : \sim P(x)$

Vale entonces la siguiente regla: para negar una función proposicional cuantificada existencialmente se cambia el cuantificar en universal, y se niega la funcion proposicional.

Se tienen las siguientes equivalencias

$$\sim[\forall x : P(x)] \Leftrightarrow \exists x / \sim P(x)$$

$$\sim[\exists x / P(x)] \Leftrightarrow \forall x : \sim P(x)$$

*Ejemplo 1-13.*

Sea la proposición:

Todo el que la conoce, la admira.

Nos interesa escribirla en lenguaje simbólico, negarla, y retraducir la negación al lenguaje ordinario.

La proposición dada puede enunciarse:

Cualquiera que sea la persona, si la conoce, entonces la admira.

Aparece clara la cuantificación de una implicación de las funciones proposicionales

$P(x)$ : $x$ la conoce
$Q(x)$ : $x$ la admira

Se tiene

$$\forall x : P(x) \Rightarrow Q(x)$$

Teniendo en cuenta la forma de negar una función proposicional cuantificada universalmente y una implicación resulta

$$\exists x / P(x) \wedge \sim Q(x)$$

Y pasando al lenguaje ordinario:

Hay personas que la conocen y no la admiran.

*Ejemplo 1-14.*

Consideremos la misma cuestión en el siguiente caso:

Todo entero admite un inverso aditivo.

Es decir

"Cualquiera que sea el entero, existe otro que sumado a él da cero".

Intervienen dos variables y la función proposicional

$$P(x, y) : x + y = 0$$

La expresión simbólica es entonces

$$\forall x\ \exists y / x + y = 0$$

Su negación es

$$\exists x / \sim [\exists y / x + y = 0]$$

Es decir

$$\exists x / \forall y : x + y \neq 0$$

La traducción al lenguaje común es

"Existe un entero cuya suma con cualquier otro, es distinta de cero". (F)

***Ejemplo 1-15.***

Sea la proposición

Hay alumnos que estudian y trabajan.

Su enunciado sugiere un cuantificador existencial y dos funciones proposicionales

$$P(x): x \text{ estudia}$$
$$Q(x): x \text{ trabaja}$$

En forma simbólica se tiene

$$\exists x / P(x) \wedge Q(x)$$

Su negación es

$$\forall x : \sim [P(x) \wedge Q(x)]$$

Y por ley de De Morgan

$$\forall x : \sim P(x) \vee \sim Q(x)$$

Traduciendo al lenguaje ordinario

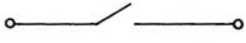
"Cualquiera que sea el alumno, no estudia o no trabaja".

## 1.11 CIRCUITOS LOGICOS

La verdad de una proposición puede asociarse al pasaje de corriente en un circuito eléctrico con un interruptor.

Para representar a $p$, si es V, se tiene

Y para $p$, si es F



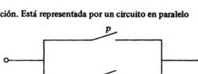
Es decir, el interruptor se cierra si $p$ es V y se abre si $p$ es F.

Las operaciones proposicionales pueden representarse mediante circuitos con tantos interruptores como proposiciones componentes, combinados en serie o paralelamente.

i ) Conjunción

Este circuito admite el pasaje de corriente, es decir, la verdad de $p \wedge q$, sólo si las dos son V.

ii ) Disyunción. Está representada por un circuito en paralelo




La falsedad de $p \vee q$, es decir, el hecho de que no pase corriente, sólo se verifica en el caso de la falsedad simultánea de $p$ y $q$.

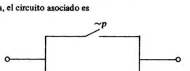
iii) Implicación. Como

$$(p \Rightarrow q) \Leftrightarrow \sim(p \wedge \sim q)$$

de acuerdo con 1.8, aplicando una ley de De Morgan y la doble negación, se tiene

$$(p \Rightarrow q) \Leftrightarrow (\sim p \vee q)$$

En consecuencia, el circuito asociado es



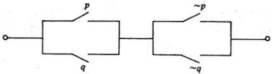

iv) Diferencia simétrica.

Utilizando sucesivamente 1.4.6., 1.4.5., una ley de De Morgan, la negación de

implicaciones y la distributividad de la disyunción respecto de la conjunción, se tienen las equivalencias

$$(p \veebar q) \Leftrightarrow \sim(p \Leftrightarrow q) \Leftrightarrow$$
$$\Leftrightarrow \sim[(p \Rightarrow q) \wedge (q \Rightarrow p)] \Leftrightarrow$$
$$\Leftrightarrow \sim(p \Rightarrow q) \vee \sim(q \Rightarrow p) \Leftrightarrow$$
$$\Leftrightarrow (p \wedge \sim q) \vee (q \wedge \sim p) \Leftrightarrow$$
$$\Leftrightarrow (p \vee q) \wedge (p \vee \sim p) \wedge (\sim q \vee q) \wedge (\sim q \vee \sim p)$$
$$\Leftrightarrow (p \vee q) \wedge (\sim p \vee \sim q)$$

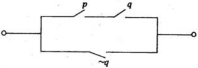
y resulta el circuito



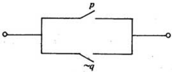

***Ejemplo 1-16.***

i ) El circuito correspondiente a la proposición

$$(p \wedge q) \vee (\sim q) \qquad \text{es}$$

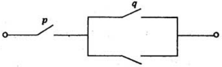



O bien, luego de simplificar aquélla: $p \vee \sim q$.




Para que pase corriente es suficiente que $p$ o $\sim q$ sean V.

ii) La operación proposicional que caracteriza al siguiente circuito




es

$$p \wedge (q \vee r)$$

## TRABAJO PRACTICO I

*1-17.* En el libro Hijos en libertad, de A. S. Neill, están escritas las siguientes proposiciones

$p$ : Mis maestros hacen que todas las lecciones sean aburridas.
$q$ : No aceptan las respuestas que no figuran en los libros.
$r$ : Imponen un cúmulo de normas estúpidas.

Construir las proposiciones

$$p \wedge q \quad , \quad \sim q \vee r \quad , \quad (p \wedge q) \Rightarrow r$$

*1-18.* Escribir en forma simbólica la siguiente proposición compuesta que figura en el mismo texto:

"La chatura y el tedio de ciertas disciplinas escolares se trasmiten a los maestros, y las escuelas se llenan de hombres y mujeres de mentalidad estrecha, vanidosos, cuyo horizonte está limitado por el pizarrón y el libro de texto".

*1-19.* Confeccionar las tablas de valores de verdad de las proposiciones

i ) $(p \wedge q) \Rightarrow r$

ii ) $\sim(p \vee q) \Leftrightarrow \sim p \wedge \sim q$

*1-20.* Negar las proposiciones construidas en el ejercicio 1-17.

*1-21.* Proponer las siguientes proposiciones en forma simbólica, negarlas, y retraducirlas al lenguaje común:

i ) No es justa, pero mantiene el orden.
ii ) Los alumnos conocen a los simuladores y los desprecian.
iii) Si los alumnos conocen a los simuladores, entonces los desprecian.

*1-22.* Determinar si las siguientes proposiciones son leyes lógicas:

i ) $p \wedge q \Rightarrow q$

ii ) $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$

iii) $p \Rightarrow p \wedge q$

iv) $p \Rightarrow p \vee q$

*1-23.* Simplificar las siguientes proposiciones:

i ) $\sim(\sim p \vee \sim q)$

ii ) $\sim(p \vee q) \vee (\sim p \wedge q)$

*1-24.* Sabiendo que $p \vee q$ es V y que $\sim q$ es V, determinar el valor de verdad de

$$[(p \vee q) \wedge \sim q] \Rightarrow q$$

*1-25.* Determinar, en cada caso, si la información que se da es suficiente para conocer el valor de verdad de las siguientes proposiciones compuestas. En caso afirmativo, justificarlo.

i ) $(p \Rightarrow q) \Rightarrow r$ ; $r$ es V

ii ) $(p \vee q) \Leftrightarrow (\sim p \wedge \sim q)$ ; $q$ es V

iii) $(p \wedge q) \Rightarrow (p \vee r)$ ; $p$ es V y $r$ es F

iv) $p \wedge (q \Rightarrow r)$ ; $p \Rightarrow r$ es V

*1-26.* Los valores de verdad de las proposiciones $p$, $q$, $r$ y $s$ son, respectivamente, V, F, F, V. Obtener los valores de verdad de

i ) $[(p \vee q) \vee r] \wedge s$

ii ) $r \Rightarrow s \wedge p$

iii) $p \vee r \Leftrightarrow r \wedge \sim s$

*1-27.* Negar las proposiciones

i ) $\exists x / P(x) \vee \sim Q(x)$

ii ) $\forall x : P(x) \Rightarrow Q(x)$

iii) $\forall x \exists y / x \cdot y = 0$

*1-28.* Verificar que para probar la equivalencia de las proposiciones $p$, $q$, $r$ y $s$ es suficiente demostrar las siguientes implicaciones:

$$p \Rightarrow q \quad , \quad q \Rightarrow r \quad , \quad r \Rightarrow s \quad \text{y} \quad s \Rightarrow p$$

*1-29.* Dadas las proposiciones

i ) El cuadrado de todo número real es mayor que 2,

ii ) Existen enteros cuyo cubo aumentado en 1 es igual al cubo del siguiente,

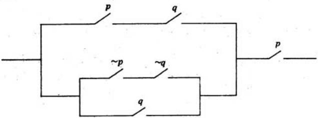
iii) Todo el que estudia triunfa,

expresarlas simbólicamente, negar las expresiones obtenidas y retraducirlas al lenguaje ordinario.

*1-30.* Construir un circuito correspondiente a la proposición

$$(p \wedge \sim q) \vee (\sim p \wedge q) \vee (\sim p \wedge \sim q)$$

**1-31.** Se tiene el siguiente circuito:




i ) determinar la proposición correspondiente

ii ) simplificar ésta, y construir el circuito asociado.

**1-32.** Expresar simbólicamente el siguiente teorema: "si un número es impar, entonces su cuadrado es impar".
Enunciar el contrarrecíproco, el contrario y el recíproco. Demostrar el primero.

**1-33.** Siendo

$$p : a \, . \, b \text{ es impar}$$
$$q : a \text{ y } b \text{ son impares}$$

Demostrar $p \Rightarrow q$

**1-34.** Justificar el razonamiento

$$\begin{array}{c} p \vee \sim q \\ \sim q \Leftrightarrow r \\ p \vee \sim r \\ \hline p \end{array}$$

**1-35.** Lo mismo en el siguiente caso:

$$\begin{array}{c} p \wedge q \\ (p \wedge q) \Rightarrow r \\ r \Rightarrow s \\ \hline s \end{array}$$

**1-36.** Investigar la validez del razonamiento siguiente:

Si el interés no es egoísta, entonces es la fuerza vital de las personas y es espontáneo.
<u>El interés no es la fuerza vital de las personas y es espontáneo</u>
El interés es egoísta

Capítulo 2

# CONJUNTOS

## 2.1. INTRODUCCION

El propósito de esta sección es el estudio de la teoría intuitiva de conjuntos. En este sentido, los términos "conjunto", "pertenencia" y "elemento" son considerados como primitivos. Sobre esta base se definen la inclusión y la igualdad, y se estudian sus propiedades. El mismo tratamiento se hace corresponder a las operaciones entre conjuntos. El capítulo se completa con el desarrollo de ejemplos en los que se pretende mostrar un método adecuado de trabajo.

## 2.2. DETERMINACION DE CONJUNTOS

### 2.2.1. Notaciones

Para denotar conjuntos utilizaremos generalmente letras mayúsculas, y para especificar elementos se usarán letras minúsculas, a menos que dichos elementos sean, a su vez, conjuntos. Para indicar la pertenencia de un elemento a un conjunto será utilizado el símbolo $\epsilon$.

La proposición "$a \in A$" se lee: "*a* pertenece a A", o bien "el elemento *a* pertenece al conjunto A".

Su negación es "$a \notin A$", que se lee: "*a* no pertenece a A".

Si el conjunto A está formado por los elementos *a, b* y *c*, escribimos

$$A = \{a, b, c\}$$

en este caso se nombran todos los elementos del conjunto, y se dice que está determinado por extensión.

Las notaciones usuales para caracterizar conjuntos numéricos son las siguientes:

N conjunto de los números naturales
Z conjunto de los números enteros

**Q** conjunto de los números racionales
**R** conjunto de los números reales
**C** conjunto de los números complejos

La representación por extensión del conjunto cuyos elementos son $-1$, 0 y 1, es

$$A = \{ -1 , 0 , 1 \}$$

Es fácil ver que se trata del conjunto de los números enteros cuyo valor absoluto es menor que 2; en este enunciado hacemos referencia a elementos del conjunto **Z**, de los números enteros, el cual se llama referencial o universal; además, estamos interesados en aquellos que satisfacen la propiedad de ser, en valor absoluto, menores que 2.

La notación correspondiente es

$$A = \{ x \in \mathbf{Z} / |x| < 2 \}$$

y se dice que el conjunto ha sido determinado por comprensión.

El conjunto universal depende de la disciplina en estudio, se fija de antemano, y está formado por todos los elementos que intervienen en el tema de interés. En general se denotará con U.

***Definición***

Un conjunto se determina por extensión si y sólo si se enumeran todos los elementos que lo constituyen. Un conjunto se define por comprensión si y sólo si se da la propiedad que caracteriza a sus elementos.

El conjunto cuyos elementos verifican la propiedad P se indica

$$A = \{ x \in U / P(x) \}$$

o más brevemente, si U está sobrentendido

$$A = \{ x / P(x) \}$$

y se lee: "A es el conjunto formado por los elementos $x$, tales que $P(x)$". $P(x)$ es una función proposicional, y un objeto del universal pertenece al conjunto si y sólo si verifica la propiedad, es decir

$$a \in A \Leftrightarrow P(a) \text{ es V}$$

En consecuencia

$$a \notin A \Leftrightarrow P(a) \text{ es F}$$

### 2.2.2. Conjuntos especiales

Extendemos la noción intuitiva de conjunto a los casos de carencia de elementos y de unicidad de elementos, mediante la introducción de los conjuntos vacío y unitario.

Un conjunto vacío es aquel que carece de elementos. Un conjunto unitario está formado por un único elemento.

Una propiedad o función proposicional, que se convierte en proposición falsa para todos los elementos del universal, caracteriza por comprensión un conjunto vacío. Designaremos con $\phi$ al conjunto vacío, y puede definirse simbólicamente así

$$\phi = \{ x / x \neq x \}$$

En este caso la propiedad relativa a $x$ es $P(x) : x \neq x$, la cual resulta falsa cualquiera que sea $x$.

Si A es el conjunto cuyo único elemento es $a$, escribiremos

$$A = \{ a \} = \{ x / x = a \}$$

*Ejemplo 2-1.*

Determinar simbólicamente y por extensión los siguientes conjuntos definidos por comprensión:

i ) A es el conjunto de los números enteros cuyo cuadrado es igual a 1

En este caso la propiedad que caracteriza a los elementos de A es la conjunción de

$$P(x) : x \in \mathbf{Z} \quad y \quad Q(x) : x^2 = 1$$

Entonces

$$A = \{ x / x \in \mathbf{Z} \wedge x^2 = 1 \}$$

y como universal puede sobrentenderse el conjunto de los números reales o racionales. Si proponemos a **Z** como universal, puede escribirse

$$A = \{ x \in \mathbf{Z} / x^2 = 1 \}$$

Obviamente, la determinación por extensión es

$$A = \{ -1 , 1 \}$$

ii ) B es el conjunto de los números naturales mayores que 2, y que no superan a 6.

Considerando a **N** como universal, la propiedad característica de los elementos de B es la conjunción de

$$P(x) : x > 2 \quad y \quad Q(x) : x \leqslant 6$$

que podemos expresar $\quad R(x) : 2 < x \leqslant 6$

y se tiene

$$B = \{ x \in \mathbf{N} / 2 < x \leqslant 6 \}$$

Por extensión nos queda

$$B=\left\{3,4,5,6\right\}$$

iii) C es el conjunto de los números reales cuyo cuadrado es igual a $-1$.

Se tiene:

$$C=\left\{x\in \mathbf{R}\,/\,x^2=-1\right\}$$

Como el cuadrado de ningún número real es negativo, $P(x): x^2=-1$ es F para todo real, y resulta $C=\phi$.

*Ejemplo 2-2.*

La determinación de conjuntos por extensión no es posible en el caso de infinitos elementos, y hay que limitarse a la definición por comprensión. La matemática trabaja casi con exclusividad en este sentido, a través de propiedades.

Caracterizamos simbólicamente los siguientes conjuntos:

i) P es el conjunto de los números enteros pares.

Por definición, un entero es par si y sólo si se identifica con el duplo de algún entero. Es decir

$$a \text{ es par} \Leftrightarrow \exists\, k\in \mathbf{Z}\,/\,a=2k$$

Entonces $$P=\left\{x\in \mathbf{Z}\,/\,x=2k \;\wedge\; k\in \mathbf{Z}\right\}$$

Es claro que P consiste en el conjunto de los múltiplos de 2.

A veces, acudiendo a un abuso de notación, suele proponerse una aparente determinación por extensión de un conjunto infinito, con la adjunción de puntos suspensivos. Así

$$P=\left\{\ldots\ldots,-4,-2,0,2,4,6,\ldots\ldots\right\}$$

ii) A es el conjunto de los números naturales que son múltiplos de 3.

$$A=\left\{x\in \mathbf{N}\,/\,x=3k \;\wedge\; k\in \mathbf{N}\right\}$$

En N no incluimos al cero, y se tiene

$$A=\left\{3,6,9,\ldots\ldots\right\}$$

Si 0 se considera natural, escribiremos $\mathbf{N}_0$ y en este caso

$$A=\left\{x\in \mathbf{N}_0\,/\,x=3k \;\wedge\; k\in \mathbf{N}_0\right\}$$

Es decir

$$A=\left\{0,3,6,9,\ldots\ldots\right\}$$

iii) B es el conjunto de los números naturales cuyo cuadrado es par.

$$B = \left\{ x \in \mathrm{N} \,/\, x^2 \ \text{ es par} \right\}$$

O bien

$$B = \left\{ x \in \mathrm{N} \,/\, x^2 = 2k \ \wedge \ k \in \mathrm{N} \right\}$$

¿Cómo se determina la pertenencia de un elemento a B? De acuerdo con la definición de B, dado un número natural, se analiza su cuadrado; si dicho cuadrado es par, el número pertenece a B; si su cuadrado es impar, no pertenece a B. Es decir

$$a \in B \Leftrightarrow a^2 \ \text{ es par}$$

iv) C es el conjunto de los puntos del plano cuyas distancias a un punto 0 son iguales a 1.

Entendemos que el conjunto universal es el de los puntos del plano $\alpha$. Si bien 0 es un elemento, como es usual en geometría, lo denotamos con mayúscula. Indicamos la distancia entre A y 0 mediante $d$ (A , 0). Entonces

$$C = \left\{ X \in \alpha \,/\, d\,(X\,,0) = 1 \right\}$$

es la definición simbólica de la circunferencia de centro 0 y radio 1.

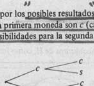
v) D es el conjunto de los puntos del plano que equidistan de dos puntos fijos A y B.

$$D = \left\{ X \in \alpha \,/\, d\,(X\,, A) = d\,(X\,, B) \right\}$$

D consiste en la mediatriz del segmento AB.

*Ejemplo 2-3.*

El conjunto S está formado por los posibles resultados que se obtienen al lanzar dos monedas. Los resultados para la primera moneda son $c$ (cara) y $s$ (sello) y por cada uno de ellos se tienen las mismas posibilidades para la segunda, es decir




Entonces

$$S = \left\{ cc\,,\, cs\,,\, sc\,,\, ss \right\}$$

## 2.3. INCLUSION

### 2.3.1. Concepto

Sean A y B dos conjuntos. Si ocurre que todo elemento de A pertenece a B, diremos que A está incluido en B, o que A es parte de B, o que A es un subconjunto de B, y escribimos $A \subset B$.

***Definición***

$$A \subset B \Leftrightarrow \forall x : x \in A \Rightarrow x \in B$$

Esta definición tiene el siguiente significado: si sabemos que $A \subset B$, entonces la proposición $\forall x : x \in A \Rightarrow x \in B$ es V; recíprocamente, si esta proposición es V, entonces se verifica que $A \subset B$.

En repetidas ocasiones se necesitará demostrar que un conjunto es parte de otro; entonces, de acuerdo con la definición, será suficiente demostrar que cualquier elemento del primero pertenece al segundo.

Teniendo en cuenta la equivalencia entre una implicación y la contrarrecíproca, la definición anterior puede expresarse así

$$A \subset B \Leftrightarrow \forall x : x \notin B \Rightarrow x \notin A$$

Además, considerando la equivalencia entre $p \Rightarrow q$ y $\sim (p \wedge \sim q)$, podemos traducir la misma definición de la siguiente manera

$$A \subset B \Leftrightarrow \exists x / x \in A \wedge x \notin B \text{ es F}$$

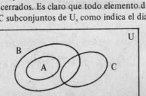
Es decir, en la inclusión no puede darse que haya un elemento de A que no pertenezca a B.

Sobrentendiendo el cuantificador universal, para descargar la notación, escribiremos

$$A \subset B \Leftrightarrow x \in A \Rightarrow x \in B$$

### 2.3.2. Diagramas de Venn

Existe una representación visual de los conjuntos dada por diagramas llamados de Venn. En este sentido, el conjunto universal suele representarse por un rectángulo, y los conjuntos por recintos cerrados. Es claro que todo elemento de A pertenece a U, es decir, $A \subset U$. Sean A, B y C subconjuntos de U, como indica el diagrama



En este caso se verifica $A \subset B$.

*Ejemplo 2-4.*

Sean $U = N$ y los conjuntos

$$A = \{ x / x \mid 6 \}$$
$$B = \{ x / x \mid 8 \}$$
$$C = \{ x / x \leqslant 2 \}$$

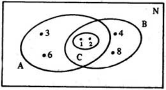
Se pide la representación de tales conjuntos mediante diagramas de Venn. Definimos la relación de divisor en N mediante

$$a \mid b \text{ si y sólo si } \exists\ n \in N / b = a \, . \, n$$

Teniendo en cuenta esta definición, y la relación de menor o igual, la representación por extensión de tales conjuntos es

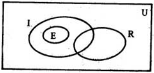
$$A = \{ 1, 2, 3, 6 \} \qquad B = \{ 1, 2, 4, 8 \}$$
$$C = \{ 1, 2 \}$$

y en términos de diagramas de Venn




*Ejemplo 2-5.*

Consideremos el conjunto U de todos los triángulos; si I denota el conjunto de los triángulos isósceles, E de los equiláteros y R de los triángulos rectángulos, se tiene



Ya que todo triángulo equilátero tiene los tres lados iguales, en consecuencia tiene dos iguales, es decir, es isósceles. Además existen triángulos isósceles que son rectángulos, pero ningún triángulo equilátero es rectángulo.

### 2.3.3. Igualdad de conjuntos

Es claro que dos conjuntos son iguales si son idénticos, es decir, si tienen los mismos elementos. Entonces, todo elemento del primero pertenece al segundo, y todo elemento de éste pertenece al primero.

*Definición*

$$A = B \Leftrightarrow A \subset B \wedge B \subset A.$$

*Ejemplo 2-6.*

Los conjuntos de números reales

$$A = \left\{ x \,/\, x^2 = x \right\}$$

$$B = \left\{ x \,/\, (x-1)\,.\,x = 0 \right\}$$

son iguales ya que

$$x \in A \Leftrightarrow x^2 = x \Leftrightarrow x^2 - x = 0 \Leftrightarrow x\,.\,(x-1) = 0 \Leftrightarrow x \in B$$

El bicondicional se desdobla en las dos implicaciones que prueban la doble inclusión, y en consecuencia la igualdad.

*Ejemplo 2-7.*

Sean los conjuntos de números enteros

$$A = \left\{ x \,/\, x^2 = 1 \right\}$$

$$B = \left\{ x \,/\, |x| = 1 \right\}$$

Teniendo en cuenta que el cuadrado de un número entero es igual al cuadrado de su valor absoluto, resulta

$$x \in A \Leftrightarrow x^2 = 1 \Leftrightarrow |x|^2 = 1 \Leftrightarrow |x| = 1 \Leftrightarrow x \in B$$

En consecuencia, $A = B$.

*Ejemplo 2-8.*

Demostrar que el conjunto de los números naturales impares es igual al conjunto de los números naturales cuyo cuadrado es impar.

Hipótesis) $A = \left\{ x \in \mathbf{N} \,/\, x \text{ es impar} \right\}$ Tesis) $A = B$

$$B = \left\{ x \in \mathbf{N} \,/\, x^2 \text{ es impar} \right\}$$

Demostración)

*Nota previa:*

Por definición, un número natural $x$ es impar si y sólo si existe $k \in \mathbf{N}$ tal que $x = 2k - 1$.

Por otra parte, es fácil ver que el producto de dos naturales consecutivos es impar, y que la diferencia entre un número par y uno impar es impar. Vamos ahora a nuestra demostración, la cual consiste en probar las dos inclusiones que definen la igualdad

1°) $A \subset B$. En efecto: sea $x \in A$.

$$\text{Se tiene } x \in A \Rightarrow x \text{ es impar} \Rightarrow x = 2k - 1 \text{ con } k \in \mathbf{N} \Rightarrow$$
$$\Rightarrow x^2 = 4k^2 - 4k + 1 \text{ con } k \in \mathbf{N} \Rightarrow x^2 = 2 \cdot (2k^2 - 2k) + 2 - 1 \Rightarrow$$
$$\Rightarrow x^2 = 2 \cdot (2k^2 - 2k + 1) - 1 \Rightarrow x^2 = 2 \cdot k' - 1 \text{ siendo } k' \in \mathbf{N} \Rightarrow$$
$$\Rightarrow x^2 \text{ es impar} \Rightarrow x \in B$$

Hemos utilizado sucesivamente, la definición de A, la definición de número impar, cuadrado de un binomio, la distributividad de la multiplicación, la sustitución de 1 por $(2 - 1)$, nuevamente la distributividad, la definición de número impar, y finalmente la definición de B.

2°) $B \subset A$. Es claro que $x = x \cdot (x + 1) - x^2$.

Ahora bien

$$x \in B \Rightarrow x^2 \text{ es impar} \Rightarrow x \cdot (x + 1) - x^2 \text{ es impar} \Rightarrow$$
$$\Rightarrow x \text{ es impar} \Rightarrow x \in A$$

En consecuencia $A = B$.

### 2.3.4. Propiedades de la inclusión

i ) REFLEXIVIDAD. Todo conjunto es parte de sí mismo.

En efecto, si A es un conjunto, la implicación

$$\forall x : x \in A \Rightarrow x \in A \text{ es V}$$

En consecuencia, por definición, se tiene $A \subset A$.

ii ) TRANSITIVIDAD. Si un conjunto es parte de otro y éste es parte de un tercero, entonces el primero está incluido en el tercero.

Hipótesis) $A \subset B$ Tesis) $A \subset C$
$B \subset C$

Demostración)

Sea $x \in A$. Por hipótesis se tiene

$$x \in A \Rightarrow x \in B$$
$$\text{y } x \in B \Rightarrow x \in C$$

Entonces, por ley del silogismo hipotético

$$x \in A \Rightarrow x \in C$$

Y, en consecuencia, por definición de inclusión $A \subset C$.

iii) ANTISIMETRIA. Si un conjunto es parte de otro y éste es parte del primero, entonces son iguales.

$$A \subset B \wedge B \subset A \Rightarrow A = B$$

es una consecuencia de la definición de igualdad.

### 2.3.5. Caracterización del conjunto vacío

i ) **Propiedad.** El conjunto vacío está incluido en cualquier otro.

Hipótesis) A es un conjunto.
Tesis) $\phi \subset A$.
Demostración) Consideramos la siguiente proposición:

$$\forall x : x \in \phi \Rightarrow x \in A$$

la cual es V por ser el antecedente F. En consecuencia, de acuerdo con la definición de inclusión, se tiene $\phi \subset A$.

*Nota:*

El teorema es válido cualquiera que sea A; en particular, A puede ser vacío.

ii ) **Propiedad.** El conjunto vacío es único.

En efecto, suponemos que, además de $\phi$, existe $\phi'$ también vacío. Entonces, de acuerdo con i ), es verdadera la proposición

$$\phi' \subset \phi \wedge \phi \subset \phi'$$

y, por definición de igualdad, resulta $\phi' = \phi$

*Ejemplo 2-9.*

Demostrar $\quad A \subset \phi \Rightarrow A = \phi$.

Como se trata de una igualdad se requieren dos inclusiones.

1°) $\phi \subset A$ por 2.3.5. i ).

2°) $A \subset \phi$. Se verifica por hipótesis.

Luego $A = \phi$.

## 2.4. CONJUNTO DE PARTES

Dado un conjunto A, podemos formar un nuevo conjunto constituido por todos los subconjuntos de A, el cual recibe el nombre de conjunto de partes de A.

***Definición***

Conjunto de partes de A es el conjunto cuyos elementos son todos subconjuntos de A.

$$P(A) = \{ X / X \subset A \}$$

Los elementos de este conjunto son a su vez conjuntos, y, en consecuencia, $P(A)$ es un conjunto de conjuntos.

De acuerdo con la definición, se tiene

$$X \in P(A) \Leftrightarrow X \subset A$$

El problema de decidir si un objeto es un elemento de $P(A)$ se reduce a determinar si dicho objeto es un subconjunto de A.

De acuerdo con la propiedad reflexiva de la inclusión, cualquiera que sea A, se tiene $A \subset A$, y en consecuencia $A \in P(A)$ por definición de conjunto de partes.

Además, por 2.3.5. i) se sabe que $\phi \subset A$, y por la misma definición $\phi \in P(A)$. Es decir, cualquiera que sea A, el mismo A y el vacío son elementos de $P(A)$.

*Ejemplo 2-10.*

Determinar el conjunto de partes de $A = \{ 2, 3, 4 \}$

Los elementos de $P(A)$ son todos los subconjuntos de A, es decir

$$\phi$$
$$\{2\}, \{3\}, \{4\}$$
$$\{2,3\}, \{2,4\}, \{3,4\}$$
$$A$$

Y la notación por extensión es

$$P(A) = \{ \phi, \{2\}, \{3\}, \{4\}, \{2,3\}, \{2,4\}, \{3,4\}, A \}$$

*Ejemplo 2-11.*

i ) El conjunto de partes del vacío es el conjunto cuyo único elemento es el vacío.

$$P(\phi) = \{ \phi \}$$

ii ) La pertenencia relaciona elemento a conjunto, mientras que la inclusión relaciona conjuntos entre sí. Desde este punto de vista, damos los valores de verdad de las siguientes proposiciones relativas al ejemplo 2-10.

| | |
|---|---|
| $\phi \subset A$ | V |
| $\phi \in A$ | F |
| $\phi \in P(A)$ | V |

$$\phi \subset P(A) \quad V$$
$$\{2,3\} \in P(A) \quad V$$
$$2 \in P(A) \quad F$$
$$\{2\} \in P(A) \quad V$$
$$A \in P(A) \quad V$$
$$A \in A \quad F$$
$$A \subset A \quad V$$

*Ejemplo 2-12.*

Si A tiene $n$ elementos, entonces $P(A)$ tiene $2^n$ elementos. Se trata de computar el número de subconjuntos de A. Uno de ellos es el vacío. Conjuntos unitarios hay exactamente $n = \binom{n}{1}$, es decir, tantos como combinaciones de $n$ elementos, de orden 1.

El número de subconjuntos de dos elementos es el de combinaciones de $n$ elementos de orden 2, es decir $\binom{n}{2}$.

Subconjuntos ternarios hay $\binom{n}{3}$.

Y así sucesivamente, hasta obtener el único subconjunto de $n$ elementos.

El número total está dado por la suma

$$1 + \binom{n}{2} + \binom{n}{3} + \ldots + \binom{n}{n-1} + 1 = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} =$$

$$= \sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} 1^i \cdot 1^{n-i} = (1+1)^n = 2^n$$

En este desarrollo hemos aplicado la fórmula del binomio de Newton, que se justificará en el Capítulo 6.

## 2.5. COMPLEMENTACION DE CONJUNTOS

Sean A y B subconjuntos de U.

### 2.5.1. Definición

Complemento de A es el conjunto formado por los elementos de U que no pertenecen a A.

El complemento de A se denotará por $A^c$; suelen usarse también A' y $\bar{A}$.

En símbolos

$$A^c = \{ x \in U / x \notin A \}$$

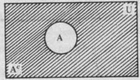
o bien

$$A^c = \{ x / x \notin A \}$$

Se tiene

$$x \in A^c \Leftrightarrow x \notin A$$

El diagrama de Venn correspondiente es




La complementación es una operación unitaria, en el sentido de que a partir de un conjunto se obtiene otro.

Es usual también obtener el complemento de un conjunto A, respecto de otro B, en cuyo caso la definición es

$$C_B A \doteq \{ x \in B / x \notin A \}$$

En particular se tiene

i ) El complementario del vacío es el universal.

$$x \in U \Rightarrow x \notin \phi \Rightarrow x \in \phi^c$$

O sea $U \subset \phi^c$

Y como $\phi^c \subset U$, resulta $\phi^c = U$

ii ) El complementario del universal es el vacío.

$$U^c = \{ x / x \in U \wedge x \notin U \} = \phi$$

### 2.5.2. Propiedades de la complementación

I) INVOLUCION. $(A^c)^c = A$

Demostración)

$$x \in (A^c)^c \Leftrightarrow x \notin A^c \Leftrightarrow \sim (x \in A^c) \Leftrightarrow \sim (x \notin A) \Leftrightarrow x \in A$$

En esta demostración hemos utilizado la definición de complemento y la ley involutiva del cálculo proposicional.

II) $A \subset B \Rightarrow B^c \subset A^c$

Demostración) Utilizando sucesivamente las definiciones de complemento, de inclusión y de complemento, se tiene

$$x \in B^c \Rightarrow x \notin B \Rightarrow x \notin A \Rightarrow x \in A^c$$

Luego $$B^c \subset A^c$$

*Ejemplo 2-13.*

Demostrar $A = B \Rightarrow A^c = B^c$

$$x \in A^c \Leftrightarrow x \notin A \Leftrightarrow x \notin B \Leftrightarrow x \in B^c$$

En virtud de las definiciones de complemento, igualdad y complemento.

*Ejemplo 2-14.*

i ) Si $r$ es una recta incluida en el plano $\alpha$, entonces su complemento es el par de semiplanos opuestos abiertos, de borde $r$.

ii ) El complementario del conjunto de los números naturales pares es el conjunto de los naturales impares.

iii) El complementario de **Q** en **R** es el conjunto de los números irracionales.

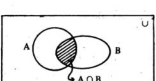
## 2.6. INTERSECCION DE CONJUNTOS

Sean A y B subconjuntos de U.

### 2.6.1. Definición

Intersección de dos conjuntos A y B es el conjunto formado por los elementos que pertenecen a A y a B.

El diagrama de Venn correspondiente es



En símbolos se tiene

$$A \cap B = \{x \in U \,/\, x \in A \ \wedge \ x \in B\}$$

O bien, sobrentendido U

$$A \cap B = \{x \,/\, x \in A \ \wedge \ x \in B\}$$

La intersección entre conjuntos es una operación binaria, porque a partir de dos conjuntos se obtiene un tercero.

La propiedad que caracteriza a los elementos de la intersección es la de pertenecer simultáneamente a los dos conjuntos, y se establece en términos de una conjunción.

La definición de intersección establece

$$x \in A \cap B \Leftrightarrow x \in A \ \wedge \ x \in B$$

Si la intersección de dos conjuntos es vacía dichos conjuntos se llaman disjuntos.

$$A \text{ y } B \text{ son disjuntos} \Leftrightarrow A \cap B = \phi$$

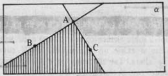
*Ejemplo 2-15.*

i ) Si $r$ y $r'$ son dos rectas distintas incluidas en un plano, entonces su intersección puede ser vacía, o bien reducirse a un punto. En el primer caso son paralelas, y en el segundo caso se llaman incidentes.

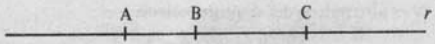
ii ) Sean dos rectas AC y AB, donde A, B y C son tres puntos no alineados pertenecientes al plano $\alpha$. Quedan definidos los conjuntos

S (AB , C) : semiplano de borde AB que pasa por C
S (AC , B) : semiplano de borde AC que pasa por B

Entonces el conjunto S (AB , C) ∩ S (AC , B) es el ángulo convexo BAC




iii) Consideremos tres puntos distintos A, B y C pertenecientes a la recta $r$:



Las semirrectas S (A , B) (de origen A que pasa por B), S (A , C) y S (C , B) son subconjuntos de $r$, tales que

$$S(A,C) \cap S(C,B) = \overline{AC}$$
$$S(A,C) \cap S(A,B) = S(A,C) = S(A,B)$$

iv) La intersección entre el conjunto de los números enteros pares y el conjunto de los números impares es vacía, ya que no existe ningún entero que sea simultáneamente par e impar.

v) En **Z**, la intersección entre el conjunto de los números pares y el conjunto de los números primos es el conjunto $\{-2, 2\}$

### 2.6.2. Propiedades de la intersección

I) IDEMPOTENCIA: $A \cap A = A$.

En efecto

$$x \in A \cap A \Leftrightarrow x \in A \ \wedge \ x \in A \Leftrightarrow x \in A$$

II) ASOCIATIVIDAD: $(A \cap B) \cap C = A \cap (B \cap C)$.

Utilizando la definición de intersección, y la asociatividad de la conjunción, se tiene

$$x \in (A \cap B) \cap C \Leftrightarrow x \in A \cap B \ \wedge \ x \in C \Leftrightarrow$$
$$\Leftrightarrow (x \in A \ \wedge \ x \in B) \ \wedge \ x \in C \Leftrightarrow x \in A \ \wedge \ (x \in B \ \wedge \ x \in C) \Leftrightarrow$$
$$\Leftrightarrow x \in A \ \wedge \ x \in B \cap C \Leftrightarrow x \in A \cap (B \cap C)$$

III) CONMUTATIVIDAD: $A \cap B = B \cap A$.

La demostración es obvia aplicando la definición de intersección y la conmutatividad de la conjunción.

IV) ELEMENTO NEUTRO PARA LA INTERSECCION ES EL UNIVERSAL.

La intersección opera sobre elementos de $P$ (U), es decir, sobre subconjuntos de U. Interesa determinar si existe un subconjunto de U cuya intersección con cualquier otro no lo altere. Tal elemento de $P$(U) se llama neutro para la intersección, y en nuestro caso es el mismo U. En efecto

cualquiera que sea $A \subset U$, se verifica $A \cap U = U \cap A = A$

*Ejemplo 2-16.*

La propiedad IV es un corolario del siguiente teorema

$$A \subset B \Leftrightarrow A \cap B = A$$

Por tratarse de una condición necesaria y suficiente realizamos las demostraciones de las dos implicaciones:

i ) $A \subset B \Rightarrow A \cap B = A$

Con la información proporcionada por la hipótesis $A \subset B$, tenemos que demostrar la igualdad $A \cap B = A$. Por definición de igualdad hemos de probar dos inclusiones:

a) Sea $x \in U$ tal que $x \in A \cap B$. Ahora bien

$$x \in A \cap B \Rightarrow x \in A \ \wedge \ x \in B \Rightarrow x \in A$$

por definición de intersección, y ley lógica $p \wedge q \Rightarrow p$.

En consecuencia $A \cap B \subset A$ (1).

La relación (1) nos dice que la intersección entre dos conjuntos está incluida en cualquiera de ellos.

b) Sea ahora

$$x \in A \Rightarrow x \in A \ \wedge \ x \in B \Rightarrow x \in A \cap B$$

por la hipótesis y por definición de intersección.

Entonces se verifica $A \subset A \cap B$ (2).

De (1) y (2) resulta $A \cap B = A$.

ii ) $A \cap B = A \Rightarrow A \subset B$

Para demostrar que $A \subset B$, consideramos

$$x \in A \Rightarrow x \in A \cap B \Rightarrow x \in A \ \wedge \ x \in B \Rightarrow x \in B$$

pues por hipótesis $A = A \cap B$; hemos utilizado además la definición de intersección y la ley lógica $p \wedge q \Rightarrow q$.

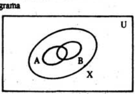
Queda probado así que $A \subset B$.

Nótese que en i ) a) no hemos hecho uso de la hipótesis, pero sí en b). Esto nos dice que la proposición $A \cap B \subset A$ es independiente de toda condición, es decir, es una propiedad intrínseca de la intersección.

*Ejemplo 2-17.*

Demostraremos que si dos conjuntos están incluidos en un tercero, entonces la intersección de los dos primeros es parte del tercero.

Esto se "ve" en el diagrama




$$A \subset X \ \wedge \ B \subset X \Rightarrow A \cap B \subset X$$

Lo demostramos así

$$x \in A \cap B \Rightarrow x \in A \ \wedge \ x \in B \Rightarrow x \in X \ \wedge \ x \in X \Rightarrow x \in X$$

Hemos aplicado sucesivamente la definición de intersección, la hipótesis y la ley lógica $p \wedge p \Rightarrow p$.

*Ejemplo 2-18.*

Demostrar que el conjunto de partes de la intersección es igual a la intersección de los conjuntos de partes.

$$P(A \cap B) = P(A) \cap P(B)$$

En efecto: teniendo en cuenta que los elementos de las partes de un conjunto son subconjuntos, consideramos

$$X \in P(A \cap B) \Leftrightarrow X \subset A \cap B \Leftrightarrow X \subset A \ \wedge \ X \subset B \Leftrightarrow X \in P(A) \ \wedge \ X \in P(B)$$
$$\Leftrightarrow X \in P(A) \cap P(B)$$

por definición de conjunto de partes; teniendo en cuenta i ) a) del ejemplo 2-16, la transitividad de la relación de inclusión, la definición de conjunto de partes y la definición de intersección.

## 2.7. UNION DE CONJUNTOS

### 2.7.1. Definición

Unión de dos conjuntos A y B es el conjunto formado por los elementos que pertenecen a A o a B.

Simbólicamente se indica

$$A \cup B = \{ x \in U / x \in A \ \vee \ x \in B \}$$

Prescindiendo del universal

$$A \cup B = \{ x / x \in A \ \vee \ x \in B \}$$

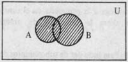
La unión de conjuntos, lo mismo que la intersección, es una operación binaria definida en el conjunto de partes de U.

De acuerdo con la definición, podemos escribir

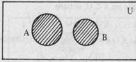
$$a \in A \cup B \Rightarrow a \in A \ \vee \ a \in B$$

El "o" utilizado es incluyente, y pertenecen a la unión aquellos elementos de U para los cuales es verdadera la disyunción; entonces un elemento pertenece a la unión si y sólo si pertenece a alguno de los dos conjuntos.

El diagrama correspondiente es




A la unión pertenecen todos los elementos de los conjuntos dados. En el caso disjunto se tiene




donde la parte sombreada es $A \cup B$.

Es claro que todo conjunto está contenido en su unión con cualquier otro. En efecto

$$x \in A \Rightarrow x \in A \ \vee \ x \in B \Rightarrow x \in A \cup B$$

en virtud de la ley lógica $p \Rightarrow p \vee q$, y de la definición de unión. Entonces

$$A \subset A \cup B \quad \text{como queríamos.}$$

*Ejemplo 2-19.*

i ) La unión de un par de rectas $r$ y $r'$ contenidas en un plano es el par de rectas.

ii ) La unión de dos semiplanos opuestos y cerrados es el plano.

iii) Sean los puntos A, B y C, como en el ejemplo 2-15, iii). Se tiene

$$S(B, A) \cup S(B, C) = r$$

$$S(A, B) \cup S(B, C) = S(A, B)$$

## 2.7.2. Propiedades de la unión

I) IDEMPOTENCIA. Cualquiera que sea A, se verifica

$$A \cup A = A$$

Pues $\quad x \in A \cup A \Leftrightarrow x \in A \ \vee \ x \in A \Leftrightarrow x \in A$

por definición de unión, y la ley lógica $p \vee p \Leftrightarrow p$.

II) ASOCIATIVIDAD. Cualesquiera que sean A, B y C

$$(A \cup B) \cup C = A \cup (B \cup C)$$

La demostración es análoga a la propuesta en el caso de la asociatividad de la intersección, utilizando ahora la definición de unión y propiedades de la disyunción.

III) CONMUTATIVIDAD. Para todo par de subconjuntos de U, se verifica

$$A \cup B = B \cup A$$

pues $x \in A \cup B \Leftrightarrow x \in A \vee x \in B \Leftrightarrow x \in B \vee x \in A \Leftrightarrow x \in B \cup A$

IV) ELEMENTO NEUTRO PARA LA UNION ES EL CONJUNTO VACIO.

Es decir, cualquiera que sea $A \subset U$, se tiene

$$A \cup \phi = \phi \cup A = A$$

Tratamos sólo el caso $A \cup \phi = A$, ya que la conmutatividad nos exime de la otra situación.

Sabemos por 2.7.1. que $A \subset A \cup \phi$ (1)

Sea ahora $x \in A \cup \phi \Rightarrow x \in A \vee x \in \phi \Rightarrow x \in A$

por definición de unión, y por ser falso $x \in \phi$.

Luego $A \cup \phi \subset A$ (2)

Por (1) y (2) resulta la igualdad propuesta.

*Ejemplo 2-20.*

Demostrar $A \subset B \Leftrightarrow A \cup B = B$.

Seguimos el mismo esquema empleado en el ejemplo 2-16.

i ) Hipótesis) $A \subset B$

Tesis) $A \cup B = B$

Demostración) Como cada conjunto está contenido en su unión con cualquier otro, según 2.7.1., se tiene

$$B \subset A \cup B \quad (1)$$

Consideremos ahora

$$x \in A \cup B \Rightarrow x \in A \vee x \in B \Rightarrow x \in B \vee x \in B \Rightarrow x \in B$$

por definición de unión, por hipótesis y por la ley $p \vee p \Rightarrow p$.

Entonces: $A \cup B \subset B$ (2)

De (1) y (2) resulta $A \cup B = B$

ii ) Hipótesis) $A \cup B = B$

Tesis) $A \subset B$

Demostración) $x \in A \Rightarrow x \in A \cup B \Rightarrow x \in B$

porque si un elemento pertenece a un conjunto, entonces pertenece a su unión con cualquiera y además por hipótesis, ya que $A \cup B = B$.

Es decir: $A \subset B$.

*Ejemplo 2-21.*

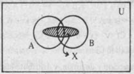
i ) Demostrar $X \subset A \ \wedge \ X \subset B \Rightarrow X \subset A \cup B$.

En efecto, sea

$$x \in X \Rightarrow x \in A \ \vee \ x \in B \Rightarrow x \in A \cup B$$

lo que es cierto por hipótesis y definición de unión.

ii ) La implicación anterior no admite recíproca verdadera, ya que puede darse que $X \subset A \cup B$, y sin embargo $X \not\subset A$ y $X \not\subset B$, como puede verse en el diagrama siguiente




iii) Demostrar $P(A) \cup P(B) \subset P(A \cup B)$.

Consideremos

$$X \in P(A) \cup P(B) \Rightarrow X \in P(A) \ \vee \ X \in P(B) \Rightarrow$$
$$\Rightarrow X \subset A \ \vee \ X \subset B \Rightarrow X \subset A \cup B \Rightarrow X \in P(A \cup B)$$

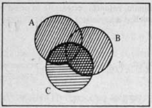
por definición de unión, de conjunto de partes, propiedad i ), y definición de conjunto de partes.

## 2.8. LEYES DISTRIBUTIVAS

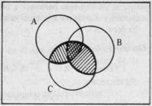
La unión e intersección de conjuntos pueden conectarse a través de dos propiedades fundamentales, llamadas leyes distributivas, que se expresan mediante las fórmulas

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$
$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

Vamos a verificar, mediante diagramas de Venn, la primera de estas leyes. Los dibujos corresponden al primero y al segundo miembro de la igualdad.




(A ∪ B) ∩ C




(A ∩ C) ∪ (B ∩ C)

Las demostraciones formales son las siguientes:

**2.8.1. Distributividad de la intersección respecto de la unión**

$$x \in (A \cup B) \cap C \Leftrightarrow x \in A \cup B \ \wedge \ x \in C \Leftrightarrow (x \in A \ \vee \ x \in B) \ \wedge \ x \in C \Leftrightarrow$$
$$\Leftrightarrow (x \in A \ \wedge \ x \in C) \ \vee \ (x \in B \ \wedge \ x \in C) \Leftrightarrow x \in A \cap C \ \vee \ x \in B \cap C \Leftrightarrow$$
$$\Leftrightarrow x \in (A \cap C) \cup (B \cap C)$$

por definiciones de intersección y de unión, y distributividad de la conjunción respecto de la disyunción.

**2.8.2. Distributividad de la unión respecto de la intersección**

$$x \in (A \cap B) \cup C \Leftrightarrow x \in A \cap B \ \vee \ x \in C \Leftrightarrow$$
$$\Leftrightarrow (x \in A \ \wedge \ x \in B) \ \vee \ x \in C \Leftrightarrow$$
$$\Leftrightarrow (x \in A \ \vee \ x \in C) \ \wedge \ (x \in B \ \vee \ x \in C) \Leftrightarrow$$
$$\Leftrightarrow x \in A \cup C \ \wedge \ x \in B \cup C \Leftrightarrow$$
$$\Leftrightarrow x \in (A \cup C) \cap (B \cup C)$$

Se han utilizado las definiciones de unión, de intersección, y la ley distributiva de la disyunción respecto de la conjunción.

## 2.9. LEYES DE DE MORGAN

Estas leyes, de gran aplicación, permiten relacionar la complementación con la unión e intersección.

**2.9.1. Teorema.** El complemento de la unión de dos conjuntos es igual a la intersección de sus complementos.

Tesis) $(A \cup B)^c = A^c \cap B^c$

Demostración) $x \in (A \cup B)^c \Leftrightarrow x \notin A \cup B \Leftrightarrow$

$$\Leftrightarrow \sim (x \in A \cup B) \Leftrightarrow \sim (x \in A \ \vee \ x \in B) \Leftrightarrow$$
$$\Leftrightarrow x \notin A \ \wedge \ x \notin B \Leftrightarrow x \in A^c \ \wedge \ x \in B^c \Leftrightarrow$$
$$\Leftrightarrow x \in A^c \cap B^c$$

Por definición de complemento, de unión, negación de una disyunción, y definición de intersección.

**2.9.2. Teorema.** El complemento de la intersección de dos conjuntos es igual a la unión de sus complementos.

Tesis) $(A \cap B)^c = A^c \cup B^c$

Demostración) $x \in (A \cap B)^c \Leftrightarrow x \notin A \cap B \Leftrightarrow$

$$\Leftrightarrow \sim (x \in A \cap B) \Leftrightarrow \sim (x \in A \ \wedge \ x \in B) \Leftrightarrow$$
$$\Leftrightarrow x \notin A \ \vee \ x \notin B \Leftrightarrow x \in A^c \ \vee \ x \in B^c \Leftrightarrow$$
$$\Leftrightarrow x \in A^c \cup B^c$$

De acuerdo con las definiciones de complemento, de intersección, negación de una conjunción y definición de unión.

*Ejemplo 2-22.*

Demostrar la equivalencia de las siguientes proposiciones:

$$A \subset B \ ; \ B^c \subset A^c \ ; \ A \cup B = B \ ; \ A \cap B = A$$

De acuerdo con lo establecido en el Capítulo 1, para demostrar la equivalencia de una cadena de $n$ proposiciones, es suficiente probar $n$ implicaciones. En nuestro caso

$$p \Rightarrow q \Rightarrow r \Rightarrow s \Rightarrow p$$

1°) $A \subset B \Rightarrow B^c \subset A^c$

En efecto $x \in B^c \Rightarrow x \notin B \Rightarrow x \notin A \Rightarrow x \in A^c$

por definición de complemento, por hipótesis y definición de complemento.

2°) $B^c \subset A^c \Rightarrow A \cup B = B$

$$\text{Sea } x \in A \cup B \Rightarrow x \in A \ \vee \ x \in B \Rightarrow$$
$$\Rightarrow x \notin A^c \ \vee \ x \in B \Rightarrow x \notin B^c \ \vee \ x \in B \Rightarrow$$
$$\Rightarrow x \in B \ \vee \ x \in B \Rightarrow x \in B$$

por definiciones de unión y de complemento, por hipótesis, definición de complemento y ley lógica $p \vee p \Rightarrow p$.

Así

$$A \cup B \subset B \qquad (1)$$

Por otra parte

$$B \subset A \cup B \qquad (2)$$

ya que todo conjunto es parte de su unión con cualquier otro.

De (1) y (2) resulta $A \cup B = B$

3°) $A \cup B = B \Rightarrow A \cap B = A$

a) Como la intersección está incluida en cualquiera de los dos conjuntos, se tiene

$$A \cap B \subset A \qquad (1)$$

b) Sea $x \in A \Rightarrow x \in A \cup B \Rightarrow x \in B$

pues $A \subset A \cup B$ y por hipótesis

Entonces

$$x \in A \Rightarrow x \in A \ \wedge \ x \in B \Rightarrow x \in A \cap B$$

Es decir $\qquad A \subset A \cap B \qquad (2)$

Por (1) y (2) resulta

$$A \cap B = A$$

4°) $A \cap B = A \Rightarrow A \subset B$

Está demostrado en el ejemplo 2-16 ii )

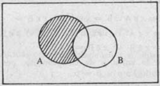
## 2.10. DIFERENCIA DE CONJUNTOS

### 2.10.1. Definición

Diferencia entre dos conjuntos A y B es el conjunto formado por los elementos de A que no pertenecen a B.

$$A - B = \left\{ x \,/\, x \in A \ \wedge \ x \notin B \right\}$$

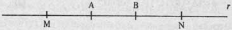
El diagrama correspondiente es




Es claro que $A - B \neq B - A$; es decir, la diferencia de conjuntos no es conmutativa.

*Ejemplo 2-23.*

i ) Considerando como universal al conjunto de los puntos del plano, la diferencia entre la recta $r$ y el segmento AB es la unión de las semirrectas abiertas AM y BN




ii ) La diferencia entre el conjunto de los números pares y el conjunto de los números primos es el conjunto de los números enteros del tipo $x = 2 \cdot k$ siendo $k \neq \pm 1$.

2.10.2. **Propiedad.** La diferencia entre dos conjuntos es igual a la intersección del primero con el complemento del segundo.

Se trata de probar que $A - B = A \cap B^c$.

En efecto, aplicando sucesivamente las definiciones de diferencia, complementación e intersección, se tiene

$$A - B = \left\{ x / x \in A \wedge x \notin B \right\} = \left\{ x / x \in A \wedge x \in B^c \right\} = A \cap B^c$$

*Ejemplo 2-24.*

Demostrar $B \subset A \Leftrightarrow (A - B) \cup B = A$

$$(A - B) \cup B = (A \cap B^c) \cup B = (A \cup B) \cap (B^c \cup B) =$$
$$= (A \cup B) \cap U = A \cup B = A$$

Por 2.10.2, distributividad de la unión respecto de la intersección, por ser $B^c \cup B = U$, por neutro para la intersección y lo demostrado en el ejemplo 2-20.

*Ejemplo 2-25.*

Demostrar la distributividad de la intersección respecto de la diferencia, es decir

$$A \cap (B - C) = (A \cap B) - (A \cap C)$$

En lugar de seguir el método general de probar las dos inclusiones, vamos a trasformar cada miembro de la igualdad utilizando las propiedades demostradas.

Así

$$A \cap (B - C) = A \cap (B \cap C^c) = A \cap B \cap C^c \qquad (1)$$

por 2.10.2 y asociatividad de la intersección. Considerando el segundo miembro y

aplicando 2.10.2, ley de De Morgan, distributividad de la intersección respecto de la unión

$$\begin{aligned}(A \cap B) - (A \cap C) &= (A \cap B) \cap (A \cap C)^c = \\ &= (A \cap B) \cap (A^c \cup C^c) = \\ &= (A \cap B \cap A^c) \cup (A \cap B \cap C^c) = \\ &= \phi \cup (A \cap B \cap C^c) = A \cap B \cap C^c \qquad (2)\end{aligned}$$

De (1) y (2) resulta

$$A \cap (B - C) = (A \cap B) - (A \cap C)$$

## 2.11. DIFERENCIA SIMETRICA

Sean A y B dos subconjuntos de U.

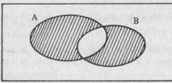
### 2.11.1. Definición

Diferencia simétrica de los conjuntos A y B es la unión de los conjuntos A − B y B − A.

La notación es

$$A \,\Delta\, B = (A - B) \cup (B - A) \qquad (1)$$

y el diagrama correspondiente




Otra identificación de la diferencia simétrica es

$$A \,\Delta\, B = (A \cap B^c) \cup (B \cap A^c) \qquad (2)$$

que se deduce como consecuencia inmediata de la definición, teniendo en cuenta que la diferencia entre dos conjuntos es igual a la intersección del primero con el complemento del segundo, según 2.10.2.

Resulta también

$$A \,\Delta\, B = (A \cup B) - (A \cap B) \qquad (3)$$

En efecto

$$A \triangle B = (A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c) =$$
$$= [(A \cap B^c) \cup B] \cap [(A \cap B^c) \cup A^c] =$$
$$= (A \cup B) \cap (B^c \cup B) \cap (A \cup A^c) \cap (B^c \cup A^c) =$$
$$= (A \cup B) \cap U \cap U \cap (A^c \cup B^c) =$$
$$= (A \cup B) \cap (A^c \cup B^c) = (A \cup B) \cap (A \cap B)^c = (A \cup B) - (A \cap B)$$

De acuerdo con (2), por ley distributiva de la unión respecto de la intersección, por ser $B^c \cup B = A \cup A^c = U$, por ser U neutro para la intersección, por conmutatividad de la unión, por ley de De Morgan y por 2.10.2.

Las expresiones alternativas para la diferencia simétrica son

$$A \triangle B = (A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c) =$$
$$= (A \cup B) - (A \cap B) = (A \cup B) \cap (A \cap B)^c$$

**2.11.2. Propiedades de la diferencia simétrica**

I) CONMUTATIVIDAD

$$A \triangle B = (A - B) \cup (B - A) = (B - A) \cup (A - B) = B \triangle A$$

II) EXISTENCIA DE NEUTRO. En $P$ (U), el vacío es neutro para la diferencia simétrica. En efecto

$$A \triangle \phi = (A - \phi) \cup (\phi - A) = A \cup \phi = A = \phi \triangle A$$

III) EXISTENCIA DE INVERSOS. En una operación entre elementos de un conjunto (en este caso el conjunto es $P$ (U), los elementos son los subconjuntos de U y la operación es la diferencia simétrica), interesa determinar si, dado un conjunto, existe otro cuya diferencia simétrica con él es el neutro. Afirmamos que todo conjunto $A \subset U$ admite al mismo A como inverso respecto de la diferencia simétrica.
En efecto

$$A \triangle A = (A - A) \cup (A - A) = \phi \cup \phi = \phi$$

IV) ASOCIATIVIDAD. Cualesquiera que sean A, B y C pertenecientes a $P$ (U) se verifica

$$(A \triangle B) \triangle C = A \triangle (B \triangle C)$$

Demostración)

$$(A \triangle B) \triangle C = [(A \triangle B) \cap C^c] \cup [(A \triangle B)^c \cap C] =$$
$$= \{ [(A \cap B^c) \cup (A^c \cap B)] \cap C^c \} \cup \{ [(A \cup B) \cap (A \cap B)^c]^c \cap C \} =$$
$$= (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup \{ [(A \cup B)^c \cup (A \cap B)] \cap C \} =$$

$$= (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C) \cup (A \cap B \cap C) =$$
$$= (A \cap B \cap C) \cup (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C) \qquad (1)$$

En este desarrollo se han utilizado las consecuencias de la definición de diferencia simétrica, leyes de De Morgan, distributividad de la intersección respecto de la unión y la conmutatividad.

Desarrollamos ahora el segundo miembro aplicando la conmutatividad de la diferencia simétrica y utilizando el resultado anterior

$$A \triangle (B \triangle C) = (B \triangle C) \triangle A =$$
$$= (B \cap C \cap A) \cup (B \cap C^c \cap A^c) \cup (B^c \cap C \cap A^c) \cup (B^c \cap C^c \cap A) =$$
$$= (A \cap B \cap C) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C) \cup (A \cap B^c \cap C^c) \qquad (2)$$

De (1) y (2) resulta

$$(A \triangle B) \triangle C = A \triangle (B \triangle C)$$

*Ejemplo 2-26.*

i ) La diferencia simétrica entre los intervalos reales

$$[1, \infty) \triangle (-\infty, 3] = (3, \infty) \cup (-\infty, 1)$$

ii ) En cambio

$$(1, \infty) \triangle (-\infty, 3) = [3, \infty) \cup (-\infty, 1]$$

*Ejemplo 2-27.*

Demostrar la ley cancelativa de la diferencia simétrica, es decir

$$A \triangle B = A \triangle C \Rightarrow B = C$$

En efecto

$$A \triangle B = A \triangle C \Rightarrow A \triangle (A \triangle B) = A \triangle (A \triangle C) \Rightarrow$$
$$\Rightarrow (A \triangle A) \triangle B = (A \triangle A) \triangle C \Rightarrow$$
$$\Rightarrow \phi \triangle B = \phi \triangle C \Rightarrow B = C$$

*Ejemplo 2-28.*

Demostrar la distributividad de la intersección respecto de la diferencia simétrica.

Tesis) $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$

Demostración) Desarrollamos los dos miembros por separado

$$(A \triangle B) \cap C = [(A \cap B^c) \cup (A^c \cap B)] \cap C =$$
$$= (A \cap B^c \cap C) \cup (A^c \cap B \cap C) \qquad (1)$$

$$(A \cap C) \Delta (B \cap C) = [(A \cap C) \cap (B \cap C)^c] \cup [(A \cap C)^c \cap (B \cap C)] =$$
$$= [(A \cap C) \cap (B^c \cup C^c)] \cup [(A^c \cup C^c) \cap (B \cap C)] =$$
$$= (A \cap C \cap B^c) \cup (A \cap C \cap C^c) \cup (A^c \cap B \cap C) \cup (C^c \cap B \cap C) =$$
$$= (A \cap B^c \cap C) \cup \phi \cup (A^c \cap B \cap C) \cup \phi =$$
$$= (A \cap B^c \cap C) \cup (A^c \cap B \cap C) \qquad (2)$$

Hemos utilizado las alternativas de la definición de diferencia simétrica, la distributividad de la intersección respecto de la unión, una ley de De Morgan, la conmutatividad de la intersección, la definición de conjuntos disjuntos y la neutralidad del $\phi$ para la unión.

## 2.12. PRODUCTO CARTESIANO

### 2.12.1 Par ordenado

Dados dos elementos $a$ y $b$ interesa formar un conjunto que dependa de dichos elementos y del orden en que se consideran.

*Definición*

Par ordenado $(a, b)$ es el conjunto cuyos elementos son $\{a\}$ y $\{a, b\}$

$$(a, b) = \{\{a\}, \{a, b\}\}$$

$a$ y $b$ son la primera y la segunda componentes del par ordenado.

En particular se tiene

$$(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$$

Si $a \neq b$, entonces $(a, b) \neq (b, a)$

Queda como ejercicio la siguiente propiedad: dos pares ordenados son iguales si y sólo si tienen sus componentes respectivamente iguales.

### 2.12.2. Definición

Producto cartesiano de dos conjuntos A y B es el conjunto cuyos elementos son todos los pares ordenados cuya primera componente pertenece a A y la segunda a B.

En símbolos

$$A \times B = \{(a, b) \,/\, a \in A \wedge b \in B\}$$

En particular

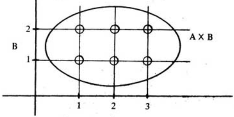
$$A \times A = A^2 = \left\{ (a, b) / a \in A \ \wedge \ b \in A \right\}$$

*Ejemplo 2-29.*

i ) Producto cartesiano de $A = \left\{ 1, 2, 3 \right\}$ y $B = \left\{ 1, 2 \right\}$

$$A \times B = \left\{ (1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2) \right\}$$

ii ) Por ser pares ordenados, los elementos del producto cartesiano de dos conjuntos pueden representarse mediante puntos del plano cuya abscisa y ordenada son, respectivamente, la primera y la segunda componente.




Los vértices de la cuadrícula obtenida son los elementos del producto cartesiano.

iii) El producto cartesiano no es conmutativo, pues

$$(3, 1) \in A \times B \ \text{y} \ (3, 1) \notin B \times A \Rightarrow$$
$$\Rightarrow A \times B \neq B \times A$$

*Ejemplo 2-30.*

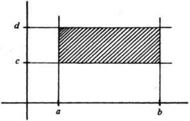
Sean los intervalos cerrados de números reales

$$[a, b] = \left\{ x \in \mathbf{R} / a \leqslant x \leqslant b \right\}$$
$$[c, d] = \left\{ y \in \mathbf{R} / c \leqslant y \leqslant d \right\}$$

Entonces

$$[a, b] \times [c, d] = \left\{ (x, y) \in \mathbf{R}^2 / a \leqslant x \leqslant b \ \wedge \ c \leqslant y \leqslant d \right\}$$

es el rectángulo cuyos lados son dichos intervalos.



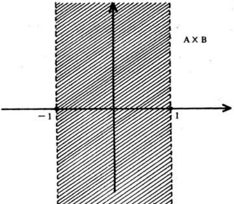

***Ejemplo 2-31.***

Sean $A = \left\{ x \in \mathbf{R} \,/\, |x| < 1 \right\}$ y $B = \mathbf{R}$

Entonces

$$A \times B = \left\{ (x, y) \in \mathbf{R}^2 \,/\, -1 < x < 1 \ \wedge \ y \in \mathbf{R} \right\}$$

es la faja abierta de la figura



***Ejemplo 2-32.***

El producto cartesiano es distributivo respecto de la unión

$$(A \cup B) \times C = (A \times C) \cup (B \times C)$$

En efecto

$$\begin{aligned}
&(x, y) \in (A \cup B) \times C \Leftrightarrow x \in A \cup B \ \wedge \ y \in C \Leftrightarrow \\
&\Leftrightarrow (x \in A \ \vee \ x \in B) \ \wedge \ y \in C \Leftrightarrow \\
&\Leftrightarrow (x \in A \ \wedge \ y \in C) \ \vee \ (x \in B \ \wedge \ y \in C) \Leftrightarrow \\
&\Leftrightarrow (x, y) \in A \times C \ \vee \ (x, y) \in B \times C \Leftrightarrow \\
&\Leftrightarrow (x, y) \in (A \times C) \cup (B \times C)
\end{aligned}$$

Hemos aplicado, sucesivamente: definiciones de producto cartesiano, de unión, distributividad de la conjunción respecto de la unión, definiciones de producto cartesiano y de unión.

El producto cartesiano de tres conjuntos se define mediante

$$A \times B \times C = (A \times B) \times C$$

Sus elementos son ternas ordenadas.

Como caso particular, se tiene

$$A^3 = A \times A \times A = \left\{ (x, y, z) / x \in A \ \wedge \ y \in A \ \wedge \ z \in A \right\}$$

En este caso, la representación es espacial.

## 2.13. OPERACIONES GENERALIZADAS

Sea $\left\{ A_1, A_2, \ldots, A_n \right\}$ un conjunto finito de conjuntos; en este caso podemos formar la unión e intersección de dicha familia, es decir

$$A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{i=1}^{n} A_i$$

$$A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i$$

donde los segundos miembros denotan abreviadamente tales operaciones.

Si consideramos $I_n = \left\{ 1, 2, \ldots, n \right\}$, entonces escribimos

$$\bigcup_{i \in I_n} A_i = \bigcup_{i=1}^{n} A_i$$

$$\bigcap_{i \in I_n} A_i = \bigcap_{i=1}^{n} A_i$$

$I_n$ es un intervalo natural inicial (conjunto de los $n$ primeros números naturales) y se llama un conjunto de índices.

Si el conjunto de índices I se identifica con N, es decir, $I = \left\{ 1, 2, 3, \ldots, n, \ldots \right\}$, entonces la familia de conjuntos $\left\{ A_1, A_2, \ldots, A_n, \ldots \right\}$ se llama sucesión de conjuntos y la notación es

$$\bigcup_{i \in I} A_i = \bigcup_{i=1}^{\infty} A_i$$

$$\bigcap_{i \in I} A_i = \bigcap_{i=1}^{\infty} A_i$$

También puede abreviarse la notación de la familia de conjuntos

$$\left\{ A_1, A_2, \ldots, A_n \right\} = \left\{ A_i \right\}_{i \in I}$$

**2.13.1.** Sea $\left\{ A_i \right\}_{i \in I}$ una familia de conjuntos.

***Definición***

Unión de la familia $\left\{ A_i \right\}_{i \in I}$ es el conjunto

$$\bigcup_{i \in I} A_i = \left\{ x \,/\, \exists\, i \in I \ \wedge \ x \in A_i \right\}$$

Es decir, un elemento pertenece a la unión de la familia si y sólo si pertenece a alguno de los conjuntos de dicha familia.

**2.13.2. Definición**

Intersección de la familia $\left\{ A_i \right\}_{i \in I}$ es el conjunto

$$\bigcap_{i \in I} A_i = \left\{ x \,/\, x \in A_i, \forall i \right\}$$

Un elemento pertenece a la intersección si y sólo si pertenece a todos los conjuntos de dicha familia.

Para las uniones e intersecciones generalizadas subsisten las propiedades del caso binario. En particular las leyes de De Morgan son

$$\left( \bigcup_{i \in I} A_i \right)^c = \bigcap_{i \in I} A_i^c$$

$$\left( \bigcap_{i \in I} A_i \right)^c = \bigcup_{i \in I} A_i^c$$

***Ejemplo. 2-33.***

Operaciones con intervalos reales

i ) $\bigcup_{i=1}^{\infty}[i-1, i) = [0,1) \cup [1,2) \cup [2,3) \cup \ldots =$

$$= \mathbb{R}^{+} \cup \{0\} = [0,\infty)$$

donde $R^+$ denota el conjunto de los números reales positivos.

ii ) $\bigcap_{i=1}^{\infty}\left(-\frac{1}{i}, \frac{1}{i}\right) = (-1,1) \cap \left(-\frac{1}{2}, \frac{1}{2}\right) \cap \ldots = \{0\}$

iii) $\bigcap_{i=1}^{\infty}\left(0, \frac{1}{i}\right) = (0,1) \cap \left(0, \frac{1}{2}\right) \cap \left(0, \frac{1}{3}\right) \cap \ldots = \phi$

## 2.14. UNIONES DISJUNTAS

En Probabilidades se utilizan uniones de conjuntos disjuntos y en lugar de utilizar las notaciones

$$A \cup B \quad \text{para el caso} \quad A \cap B = \phi$$

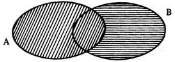
es usual escribir

$$A + B$$

símbolo que indica una unión disjunta.

Si se tiene una unión arbitraria de conjuntos, ésta puede expresarse como unión disjunta de la siguiente manera

$$A \cup B = A + A^c \cap B$$




Consideremos ahora la unión de tres conjuntos $A_1$, $A_2$ y $A_3$; la podemos expresar como unión disjunta mediante

$$\bigcup_{i=1}^{3} A_i = A_1 + A_1^c \cap A_2 + A_1^c \cap A_2^c \cap A_3$$

Indicando con el símbolo $\Sigma$ la unión en el caso disjunto, la expresión anterior en el caso de una sucesión de conjuntos puede escribirse así

$$\bigcup_{i \in N} A_i = A_1 + \sum_{j=2}^{\infty} A_1^c \cap A_2^c \cap \ldots \cap A_{j-1}^c \cap A_j$$

Se trata de probar esta igualdad.

a) El segundo miembro es una unión disjunta.

Sean dos términos de la sumatoria con $i \neq j$, por ejemplo: $i < j$. Se tiene

$$(A_1^c \cap \ldots \cap A_{i-1}^c \cap A_i) \cap (A_1^c \cap \ldots \cap A_i^c \cap \ldots \cap A_{j-1}^c \cap A_j) =$$
$$= \phi \text{ pues } A_i \cap A_i^c = \phi$$

b) Todo elemento del primer miembro pertenece al segundo.

$$\text{Sea } \; x \in \bigcup_{i \in N} A_i \Rightarrow \exists\, i \in N \,/\, x \in A_i$$

Si $k$ es el menor entero positivo para el cual $x \in A_k$, se tiene $x \notin A_1 \cup A_2 \cup \ldots \cup A_{k-1}$ ya que $x$ no pertenece a ningún $A_i$ con $i < k$.

Luego

$$x \in (A_1 \cup A_2 \cup \ldots \cup A_{k-1})^c \Rightarrow$$
$$\Rightarrow x \in A_1^c \cap A_2^c \cap \ldots \cap A_{k-1}^c \text{ y como } x \in A_k \Rightarrow$$
$$\Rightarrow x \in A_1^c \cap A_2^c \cap \ldots \cap A_{k-1}^c \cap A_k$$

y en consecuencia $x$ pertenece al segundo miembro.

c) Sea ahora un elemento del segundo miembro. Por ser una unión disjunta, dicho elemento pertenece a uno y sólo uno de los términos, es decir

$$\exists\, k \,/\, x \in A_1^c \cap A_2^c \cap \ldots \cap A_{k-1}^c \cap A_k \Rightarrow$$
$$\Rightarrow x \in A_k \text{ para un único } k \Rightarrow$$
$$\Rightarrow x \in \bigcup_{i \in N} A_i$$

## TRABAJO PRACTICO II

*2-34.* Se considera un experimento aleatorio consistente en lanzar tres monedas. Si una moneda cae cara, se anota 1, y si cae sello se anota 0. Formar el conjunto cuyos elementos son los posibles resultados del experimento.

*2-35.* Con relación al ejercicio anterior, determinar por extensión los siguientes subconjuntos:

$S_1$ : se dan más caras que sellos.

$S_2$ : se obtienen al menos dos caras.

$S_3$ : se obtiene el mismo resultado en las tres monedas.

*2-36.* Con los conjuntos definidos en 2-30, obtener:

$$S_2^c \; ; S_2 - S_3 \; ; S_1 \cap S_3 \; ; (S_2 \cup S_3) \cap S_1$$

*2-37.* Sean los conjuntos

$$A = \left\{ x \in \mathbf{Z} \,/\, |x| \leqslant 3 \right\}$$
$$B = \left\{ x \in \mathbf{Z} \,/\, x^2 < 7 \right\}$$

determinar $A \cap B$, $A \cup B$, $A - B$, $B - A$, $A \Delta B$

*2-38.* Dados

$$A = \left\{ x \in \mathbf{R} \,/\, \left| x - \frac{1}{2} \right| \leqslant 2 \right\}$$
$$B = \left\{ x \in \mathbf{R} \,/\, \left| x - 1 \right| \leqslant \frac{3}{2} \right\}$$

Obtener $A \cap B$, $A \cup B$, $B^c$

*2-39.* Siendo

$$A = \left\{ x \in \mathbf{R} \,/\, x^2 - 1 = 0 \right\}$$
$$B = \left\{ x \in \mathbf{R} \,/\, |x| \leqslant 1 \right\}$$

obtener $A \cap B$, $(A \cup B)^c$

*2-40.* Si

$$A = \left\{ x \in \mathbf{Z} \,/\, |x| < 4 \right\} \quad \text{y}$$
$$B = \left\{ x \in \mathbf{Z} \,/\, x | 6 \right\} \quad \text{determinar}$$

$$A \cup B\,,\, A \cap B\,,\, A - B\,,\, B - A\,,\, A \,\Delta\, B$$

*2-41.* Formar todos los subconjuntos de

$$A = \left\{ (0{,}0)\,,\,(1{,}0) \right\}$$

*2-42.* Siendo $A = \left\{ a\,,b \right\}$ , obtener $P(A^2)$

*2-43.* Demostrar

$$(A \cap B) \subset A \subset (A \cup B)$$

*2-44.* Demostrar

$$A \subset B \;\wedge\; A \subset C \Rightarrow A \subset (B \cap C)$$

*2-45.* Demostrar que si dos conjuntos están incluidos en un tercero, entonces su unión también lo está.

*2-46.* Demostrar

$$A \subset \phi \Rightarrow A = \phi$$

*2-47.* Demostrar

$$A - B = A - (A \cap B) = (A \cup B) - B$$

*2-48.* Demostrar

$$(A \cup B) - C = (A - C) \cup (B - C)$$

*2-49.* Demostrar

$$(A \cap B) - C = (A - C) \cap (B - C)$$

*2-50.* Demostrar

$$(A - B) - C = A - (B \cup C)$$

*2-51.* Demostrar

$$A - (B - C) = (A - B) \cup (A \cap C)$$

*2-52.* Demostrar

$$(A - B) - C \subset A - (B - C)$$

*2-53.* Demostrar

$$A \cup (B - C) = (A \cup B) - (C - A)$$

*2-54.* Demostrar

$$A = (A \cap B) \cup (A \cap B^c)$$

*2-55.* Demostrar

$$B \subset A \Leftrightarrow (A - B) \cup B = A$$

*2-56.* Demostrar

$$(A - B) \cup B = A \cup B$$

*2-57.* Demostrar

$$A \Delta B = \phi \Leftrightarrow A = B$$

*2-58.* Demostrar

$$A \times B = \phi \Leftrightarrow A = \phi \ \vee \ B = \phi$$

*2-59.* Demostrar

$$A \subset B \ \wedge \ C \subset D \Leftrightarrow A \times C \subset B \times D$$

*2-60.* Demostrar

$$(A \cap B) \times C = (A \times C) \cap (B \times C)$$

*2-61.* Demostrar

$$(A - B) \times C = (A \times C) - (B \times C)$$

*2-62.* Demostrar

i) $A \subset B \Rightarrow (A \cup C) \subset (B \cup C)$

ii) $A \subset B \Rightarrow (A \cap C) \subset (B \cap C)$

*2-63.* Demostrar

$$A \subset B \ \wedge \ A \subset C \Leftrightarrow A \subset (B \cap C)$$

*2-64.* Demostrar

$$A \subset C \ \wedge \ B \subset C \Leftrightarrow (A \cup B) \subset C$$

*2-65.* Demostrar

$$A \cap B = \phi \ \wedge \ A \cup B = C \Rightarrow A = C - B$$

*2-66.* Demostrar

i ) $U^c = \phi$

ii ) $U = \phi^c$

iii) $A \cap A^c = \phi$

iv) $A \cup A^c = U$

*2-67.* Demostrar

$$A \cup B = U \ \wedge \ A \cap B = \phi \Rightarrow B = A^c$$

**2-68.** Demostrar

$$\text{i) } A-(A-B)=A\cap B$$
$$\text{ii) } A\cup(B-A)=A\cup B$$

**2-69.** Demostrar la equivalencia de

$$A\cup B=U \quad y \quad A^c\subset B$$

**2-70.** Demostrar la equivalencia de

$$A\subset B^c \quad y \quad A\cap B=\phi$$

**2-71.** Si A tiene $n$ elementos escribimos $C(A)=n$ (cardinal de A es igual a $n$). Si A y B son finitos, entonces el cardinal de la unión es igual a la suma de los cardinales, menos el cardinal de la intersección, es decir

$$C(A\cup B)=C(A)+C(B)-C(A\cap B)$$

Demostrar

$$C(A\cup B\cup C)=C(A)+C(B)+C(C)-C(A\cap B)-$$
$$-C(A\cap C)-C(B\cap C)+C(A\cap B\cap C)$$

**2-72.** Sean $U\neq\phi$ y $\mathcal{A}$ una familia no vacía de subconjuntos de U, es decir: $\mathcal{A}\subset \mathcal{P}(U)$.

Por definición, $\mathcal{A}$ es un álgebra de Boole de partes de U, si y sólo si $\mathcal{A}$ es cerrada para la complementación, para la unión, y contiene al vacío. Es decir

i) $A\in\mathcal{A}\Rightarrow A^c\in\mathcal{A}$

ii) $A_i\in\mathcal{A},\, i\in I \Rightarrow \bigcup_{i\in I} A_i\in\mathcal{A}$

iii) $\phi\in\mathcal{A}$

donde I denota un conjunto de índices a lo sumo numerable.

Demostrar que $\mathcal{A}$ contiene a U, y que es cerrado para la intersección.

**2-73.** Sean: $\Omega\neq\phi$, $\mathcal{A}$ y $\mathcal{B}$ dos álgebras de Boole de partes de $\Omega$. Demostrar que $\mathcal{A}\cap\mathcal{B}$ es un álgebra de Boole.

Capítulo 3

# RELACIONES

## 3.1 INTRODUCCION

Se desarrolla aquí un tema de fundamental importancia en el esquema de la matemática actual: las relaciones binarias. Mediante ellas es posible vincular elementos de dos conjuntos, no necesariamente diferentes, y según sea el tipo de conexión se tienen las distintas clases de relaciones. En este capítulo se estudiarán con adecuado detalle las relaciones de equivalencia y de orden.

## 3.2. RELACIONES BINARIAS

Sean A y B dos conjuntos y P $(x , y)$ una propiedad relativa a los elementos $x \in A$ e $y \in B$, en ese orden. Esto sugiere naturalmente la consideración del producto cartesiano AXB, y la determinación de los pares ordenados $(a , b)$ para los cuales P $(a , b)$ es una proposición verdadera. De este modo queda definido un subconjunto $R \subset AXB$, llamado relación.

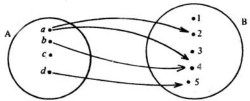
Para fijar ideas consideremos el conjunto A formado por las personas $a, b, c$ y $d$, y el conjunto B cuyos elementos son las posibles notas semanales obtenidas en una asignatura: 1, 2, 3, 4 y 5, correspondientes a insuficiente, aprobado, bueno, distinguido y sobresaliente. Es decir

$$A = \{ a , b , c , d \} \quad y \quad B = \{ 1 , 2 , 3 , 4 , 5 \}$$

Los elementos de A quedan vinculados con los del conjunto B mediante la propiedad

P $(x , y)$ : $x$ obtuvo la nota $y$

Supongamos que la situación al cabo de una semana queda especificada mediante el siguiente diagrama




Esta relación entre A y B está caracterizada por el conjunto de pares ordenados

$$R = \{ (a, 2), (a, 4), (b, 4), (d, 5) \}$$

como $c$ no tiene ningún correspondiente en B, consideramos que no ha sido clasificado en la semana. Se tiene

$$(x, y) \in R \Leftrightarrow P(x, y) \text{ es } V$$

***Definición***

Relación entre A y B es todo subconjunto del producto cartesiano A×B. En símbolos

$$R \text{ es una relación entre A y B} \Leftrightarrow R \subset A \times B$$

Para indicar que un par ordenado $(a, b)$ pertenece a la relación suele escribirse $a R b$, lo que equivale a $(a, b) \in R$.

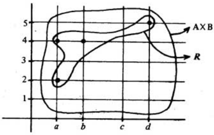
## 3.3. REPRESENTACION DE RELACIONES

Sea $R$ una relación entre A y B, es decir, $R \subset A \times B$. En el caso de conjuntos finitos se utilizan los siguientes tipos de representación:

i ) Mediante diagramas de Venn, como en el ejemplo anterior.

ii ) Mediante un gráfico cartesiano. En este caso se consideran como abscisas los elementos del primer conjunto, y como ordenadas los del segundo. Mediante paralelas a los ejes trazadas por los puntos de división se forma una cuadrícula cuyos vértices son los elementos del producto cartesiano A×B; de éstos se señalan los que pertenecen a $R$.

Considerando el ejemplo propuesto en 3.2, se tiene:




iii) Mediante un matriz. Sobre una columna se anotan los elementos de A, y sobre una fila los de B. En el ángulo superior izquierdo, el significado de la relación. Se asigna a cada elemento del producto cartesiano A×B un 1 o bien un 0, según que el par ordenado correspondiente pertenezca o no a la relación. Con el mismo ejemplo, resulta

| $R$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $a$ | 0 | 1 | 0 | 1 | 0 |
| $b$ | 0 | 0 | 0 | 1 | 0 |
| $c$ | 0 | 0 | 0 | 0 | 0 |
| $d$ | 0 | 0 | 0 | 0 | 1 |

## 3.4. DOMINIO, IMAGEN, RELACION INVERSA

Consideremos una relación $R$ entre los conjuntos A y B.

Si $(x\ ,\ y) \in R$ diremos que $y$ es una imagen de $x$ a través de $R$, y que $x$ es un antecedente o preimagen de $y$ por $R$.

*Definición*

Dominio de $R$ es la totalidad de los elementos de A, que admiten imagen en B

$$D_R = \left\{ x \in A \,/\, (x, y) \in R \right\}$$

***Definición***

Imagen de $R$ es el conjunto de los elementos de B, que admiten un antecedente en A

$$I_R = \{ y \in B \,/\, (x, y) \in R \}$$

***Definición***

Relación inversa de $R$ es el subconjunto de B×A definido por

$$R^{-1} = \{ (y, x) \,/\, (x, y) \in R \}$$

***Ejemplo 3-1.***

Con relación al caso estudiado en 3.2, se tiene

$$D_R = \{ a, b, d \} \qquad I_R = \{ 2, 4, 5 \}$$

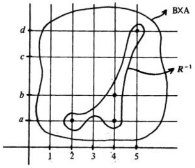
La relación inversa es

$$R^{-1} = \{ (2, a), (4, a), (4, b), (5, d) \}$$

y corresponde a la propiedad

P $(y, x)$ : $y$ es la nota obtenida por $x$

El gráfico cartesiano de esta relación inversa es



## 3.5. COMPOSICION DE RELACIONES

A partir de las relaciones $R \subset A \times B$ y $S \subset B \times C$, es posible definir una relación entre A y C, llamada composición entre $R$ y $S$, mediante

$$S \circ R = \{ (x, z) / \exists\, y \in B \wedge (x, y) \in R \wedge (y, z) \in S \}$$

La composición de relaciones admite las siguientes propiedades:

i ) Asociatividad.

$$(T \circ S) \circ R = T \circ (S \circ R)$$

ii ) La relación inversa de la composición es igual a la composición de las relaciones inversas, en orden permutado.

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$$

Las demostraciones quedan como ejercicios.

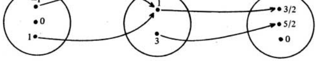
***Ejemplo 3-2.***

Consideremos los siguientes conjuntos y relaciones:

$$A = \{ -1, 0, 1 \} \qquad B = \{ 1, 3 \} \qquad C = \{ 3/2, 5/2, 0 \}$$

$R \subset A \times B$ está definida por: la imagen de $x$ es su cuadrado.

$S \subset B \times C$ caracterizada por: el correspondiente de $y$ es su mitad aumentada en 1.




Se tiene:

$$R = \{ (-1, 1), (1, 1) \}$$

$$S = \left\{ \left(1, \frac{3}{2}\right), \left(3, \frac{5}{2}\right) \right\}$$

$$S \circ R = \left\{ \left(-1, \frac{3}{2}\right), \left(1, \frac{3}{2}\right) \right\}$$

La relación compuesta $S \circ R \subset A \times C$ está determinada así:

$$(x , z) \in S \circ R \Leftrightarrow z = \frac{x^2}{2} + 1$$

### 3.6. RELACIONES DEFINIDAS EN UN CONJUNTO

Sea $R$ una relación entre A y B, donde B = A. En este caso la relación está definida en A, y se identifica con un subconjunto de $A^2 = A \times A$.

***Definición***

$R$ es una relación definida en A, si y sólo si $R \subset A^2$.

Como todo subconjunto de $A^2$ es un elemento de las partes de $A^2$, podemos decir:

$R$ es una relación definida en A si y sólo si $R \in P(A^2)$

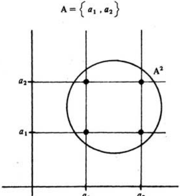
Es claro que el conjunto vacío y el mismo $A^2$ son relaciones definidas en todo conjunto A, ya que son subconjuntos de $A^2$.

Si A tiene $n$ elementos, entonces $A^2$ tiene $n^2$ elementos, y el conjunto de partes de $A^2$ tiene $2^{(n^2)}$ elementos, es decir, existen $2^{(n^2)}$ subconjuntos de $A^2$, o lo que es lo mismo, relaciones en A.

***Ejemplo 3-3.***

Se trata de formar todas las relaciones que es posible definir en el conjunto

$$A = \left\{ a_1 , a_2 \right\}$$



Determinamos primero el producto cartesiano

$$A^2 = \left\{ (a_1, a_1), (a_1, a_2), (a_2, a_1), (a_2, a_2) \right\}$$

Como $A^2$ tiene cuatro elementos, existen $2^4$ relaciones en A, y son las siguientes:

$$R_1 = \phi$$
$$R_2 = \left\{ (a_1, a_1) \right\}$$
$$R_3 = \left\{ (a_1, a_2) \right\}$$
$$R_4 = \left\{ (a_2, a_1) \right\}$$
$$R_5 = \left\{ (a_2, a_2) \right\}$$
$$R_6 = \left\{ (a_1, a_1), (a_1, a_2) \right\}$$
$$R_7 = \left\{ (a_1, a_1), (a_2, a_1) \right\}$$
$$R_8 = \left\{ (a_1, a_1), (a_2, a_2) \right\}$$
$$R_9 = \left\{ (a_1, a_2), (a_2, a_1) \right\}$$
$$R_{10} = \left\{ (a_1, a_2), (a_2, a_2) \right\}$$
$$R_{11} = \left\{ (a_2, a_1), (a_2, a_2) \right\}$$
$$R_{12} = \left\{ (a_1, a_1), (a_1, a_2), (a_2, a_1) \right\}$$
$$R_{13} = \left\{ (a_1, a_1), (a_1, a_2), (a_2, a_2) \right\}$$
$$R_{14} = \left\{ (a_1, a_1), (a_2, a_1), (a_2, a_2) \right\}$$
$$R_{15} = \left\{ (a_1, a_2), (a_2, a_1), (a_2, a_2) \right\}$$
$$R_{16} = A^2$$

***Ejemplo 3-4.***

Gráfico cartesiano de la relación definida en **R**, mediante

$$(x, y) \in R \Leftrightarrow x^2 = y^2 \qquad (1)$$

La relación es un subconjunto de $\mathbf{R}^2$, y pertenecen a ella los pares ordenados de números reales que satisfacen a (1). Ahora bien

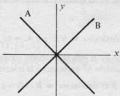
$$x^2 = y^2 \Leftrightarrow x^2 - y^2 = 0 \Leftrightarrow (x + y) \cdot (x - y) = 0$$

Sabemos que en **R**, si el producto de dos factores es cero, alguno de los factores es nulo, es decir

$$x+y=0 \ \vee \ x-y=0 \Leftrightarrow y=-x \ \vee \ y=x$$

Cada una de estas ecuaciones es la representación analítica de una recta del plano; en este caso, se trata del par de bisectrices del sistema de ejes.

$$\text{Si } A=\{(x,y)\,/\,y=-x\} \quad \text{y } B=\{(x,y)\,/\,y=x\}$$




entonces la relación

$$R=\{(x,y)\,/\,x^2=y^2\}=A\cup B, \text{ es decir es la unión de ambas bisectrices.}$$

## 3.7. POSIBLES PROPIEDADES DE LAS RELACIONES DEFINIDAS EN UN CONJUNTO

Sea $R$ una relación definida en A, es decir, $R\subset A^2$. Dicha relación puede clasificarse de acuerdo con las siguientes propiedades:

### 3.7.1. Reflexividad

$$R \text{ es reflexiva} \Leftrightarrow \forall x: x\in A \Rightarrow (x,x)\in R$$

La reflexividad de $R$ se caracteriza porque todo elemento de A forma pareja consigo mismo, y el par así obtenido pertenece a la relación.

Llamamos diagonal de $A^2$ al conjunto $D=\{(x,x)\,/\,x\in A\}$ es decir, la diagonal de $A^2$ es el conjunto de los pares de componentes iguales. La reflexividad se traduce en el hecho siguiente: la diagonal de $A^2$ está contenida en la relación, es decir

$$R \text{ es reflexiva} \Leftrightarrow D\subset R$$

### 3.7.2. No reflexividad

Consiste en la negación de 3.7.1.

$$R \text{ es no reflexiva} \Leftrightarrow \exists\, x \,/\, x \in A \;\wedge\; (x\,,x) \notin R$$

La no reflexividad de $R$ queda especificada por la existencia de al menos un elemento de A que no esté relacionado consigo mismo.

En un diagrama cartesiano ocurre que la diagonal de $A^2$ no está contenida en la relación, o sea:

$$R \text{ es no reflexiva} \Leftrightarrow R \cap D \neq D$$

### 3.7.3. Arreflexividad

$$R \text{ es arreflexiva} \Leftrightarrow \forall\, x\colon x \in A \Rightarrow (x\,,x) \notin R$$

Es decir, ningún elemento de A está relacionado consigo mismo, o lo que es igual, ningún elemento de la diagonal de $A^2$ pertenece a la relación o equivalentemente

$$R \text{ es arreflexiva} \Leftrightarrow R \cap D = \phi$$

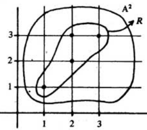
Es claro que toda relación arreflexiva es no reflexiva.

*Ejemplo 3-5.*

En $A = \{1\,,2\,,3\}$ consideramos las siguientes relaciones:

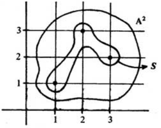
i ) $R = \{(1\,,1)\,,(2\,,2)\,,(3\,,3)\,,(2\,,3)\}$

De acuerdo con la definición dada en 3.7.1., resulta $R$ una relación reflexiva



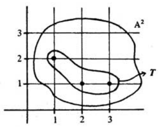

ii ) En cambio $S = \{(1\,,1)\,,(2\,,3)\,,(3\,,2)\}$ es no reflexiva, pues

$$2 \in A \;\wedge\; (2\,,2) \notin R$$




iii) $T = \{ (1, 2), (2, 1), (3, 1) \}$

Es arreflexiva, ya que ningún elemento de A forma pareja consigo mismo en la relación.




### 3.7.4. Simetría

$$R \text{ es simétrica} \Leftrightarrow \forall x \, \forall y \in A: (x, y) \in R \Rightarrow (y, x) \in R$$

Es decir, si un par pertenece a la relación, el par que resulta de permutar sus componentes también pertenece, y en consecuencia el diagrama cartesiano es simétrico respecto de la diagonal de $A^2$.

### 3.7.5. No simetría

Es la negación de la simetría.

$$R \text{ es no simétrica} \Leftrightarrow \exists x \, \exists y \,/\, (x, y) \in R \;\wedge\; (y, x) \notin R$$

La no simetría no impide que dos pares de componentes permutadas pertenezcan a la relación, pero exige que haya al menos un par en la relación, y que el que resulta de permutar sus componentes no pertenezca a ella.

### 3.7.6.-Asimetría

$$R \text{ es asimétrica} \Leftrightarrow \forall x \, \forall y : (x , y) \in R \Rightarrow (y , x) \notin R$$

En este caso debe ocurrir que si un par pertenece a la relación, entonces el que se deduce por permutación no pertenece.

*Ejemplo 3-6.*

En $A = \{1 , 2 , 3\}$ clasificamos desde este punto de vista las relaciones:

i ) $S = \{(1 , 1) , (2 , 3) , (3 , 2)\}$

es simétrica.

ii ) $T = \{(1 , 2) , (2 , 1) , (3 , 1)\}$

es no simétrica, ya que

$$(3 , 1) \in T \ \wedge \ (1 , 3) \notin T$$

iii) $U = \{(1 , 2) , (1 , 3) , (2 , 3)\}$

es una relación asimétrica en A.

### 3.7.7. Transitividad

$$R \text{ es transitiva} \Leftrightarrow \forall x \, \forall y \, \forall z : (x , y) \in R \ \wedge \ (y , z) \in R \Rightarrow (x , z) \in R$$

Es decir, si un elemento está relacionado con otro (no necesariamente distinto), y éste está relacionado con un tercero, entonces el primero está relacionado con el tercero.

### 3.7.8. No transitividad

Por ser la negación de la transitividad, decimos

$$R \text{ es no transitiva} \Leftrightarrow \exists x \, \exists y \, \exists z \, / \, (x, y) \in R \ \wedge \ (y , z) \in R \ \wedge \ (x , z) \notin R$$

### 3.7.9. Atransitividad

$$R \text{ es atransitiva} \Leftrightarrow \forall x \, \forall y \, \forall z : (x , y) \in R \ \wedge \ (y , z) \in R \Rightarrow (x , z) \notin R$$

*Ejemplo 3-7.*

Considerando el mismo conjunto A de los ejemplos 3-5 y 3-6 se tiene:

i ) $R$ y $U$ son transitivas.

ii) $V = \left\{ (1,2), (2,3), (1,3), (3,1) \right\}$ es no transitiva, ya que

$$(1,3) \in V \ \wedge \ (3,1) \in V \ \wedge \ (1,1) \notin V$$

iii) $W = \left\{ (1,2), (2,3) \right\}$ es atransitiva, ya que

$$(1,2) \in W \ \wedge \ (2,3) \in W \Rightarrow (1,3) \notin W$$

### 3.7.10. Antisimetría

$$R \text{ es antisimétrica} \Leftrightarrow \forall x \, \forall y : (x, y) \in R \ \wedge \ (y, x) \in R \Rightarrow x = y$$

En este caso, si dos pares de componentes permutadas pertenecen a la relación, entonces dichas componentes se identifican.

De este modo, la relación $R$ del ejemplo 3-5 es antisimétrica, pero no lo es $S$ puesto que es F la proposición

$$(2,3) \in S \ \wedge \ (3,2) \in S \Rightarrow 2 = 3$$

***Ejemplo 3-8.***

En **R** se considera la relación $R$ definida por

$$(x, y) \in R \Leftrightarrow x - y \in \mathbf{Z} \qquad (1)$$

Estamos interesados en la clasificación y representación de $R$.

La definición (1) se traduce en estos términos: dos reales están relacionados, si y sólo si su diferencia es un entero.

i ) Reflexividad.

$$a \in \mathbf{R} \Rightarrow a - a = 0 \in \mathbf{Z} \Rightarrow (a, a) \in R$$

ii ) Simetría.

$$(a, b) \in R \Rightarrow a - b \in \mathbf{Z} \Rightarrow b - a \in \mathbf{Z} \Rightarrow (b, a) \in R$$

Por (1), porque si un número es entero, su opuesto también lo es, y por (1)

iii) Transitividad.

$$(a, b) \in R \ \wedge \ (b, c) \in R \Rightarrow a - b \in \mathbf{Z} \ \wedge \ b - c \in \mathbf{Z} \Rightarrow$$
$$\Rightarrow (a - b) + (b - c) \in \mathbf{Z} \Rightarrow a - c \in \mathbf{Z} \Rightarrow (a, c) \in R$$

iv) $R$ no es antisimétrica, pues

$$(3,2) \in R \ \wedge \ (2,3) \in R \Rightarrow 2 = 3 \ \text{ es F}$$

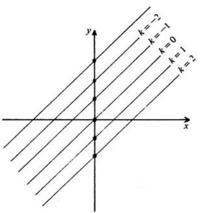
v ) Gráfico de $R$.

A $R$ pertenecen los pares de reales $(x, y)$ tales que $x - y \in \mathbf{Z}$

Ahora bien

$$x - y \in \mathbf{Z} \Rightarrow x - y = k / k \in \mathbf{Z} \Rightarrow y = x - k \quad \text{con} \quad k \in \mathbf{Z}$$

Para cada entero $k$ se tiene una recta paralela a la primera bisectriz.




La relación consiste en todos los pares $(x, y) \in \mathbf{R}^2$ pertenecientes a la familia de rectas, es decir:

$$R = \bigcup_{k \in \mathbf{Z}} \left\{ (x, y) \in \mathbf{R}^2 \,/\, y = x - k \right\}$$

*Ejemplo 3-9.*

Sea A un conjunto. Como el vacío es parte de cualquier otro, la proposición $\phi \subset A^2$ es verdadera y en consecuencia, $\phi$ es una relación en A. Tal relación verifica las propiedades:

i ) **Arreflexividad**. La proposición

$$\forall x : x \in A \Rightarrow (x, x) \notin \phi$$

es verdadera, ya que el consecuente de la implicación es V.

ii ) **Simetría**. Se verifica por ser V la proposición

$$\forall x \, \forall y : (x, y) \in \phi \Rightarrow (y, x) \in \phi$$

iii) **Transitividad**

$$(x, y) \in \phi \ \wedge \ (y, z) \in \phi \Rightarrow (x, z) \in \phi$$

es V porque el antecedente es F.

iv) Como la implicación

$$(x, y) \in \phi \ \wedge \ (y, z) \in \phi \Rightarrow x = y$$

es verdadera por tener el antecedente falso, la relación es antisimétrica.

Es decir, la relación vacía definida en un conjunto, es arreflexiva, simétrica, transitiva, y antisimétrica.

Si $A = \phi$, entonces la misma relación es además reflexiva, pues

$$\forall x : x \in A \Rightarrow (x, x) \in \phi$$

es verdadera.

## 3.8. RELACIONES DE EQUIVALENCIA

Las relaciones binarias definidas en un conjunto, que verifican las propiedades reflexiva, simétrica y transitiva, se llaman de equivalencia y desempeñan un papel importante en álgebra.

### 3.8.1. Concepto de relación de equivalencia

***Definición***

La relación $R \subset A^2$ es de equivalencia en A si y sólo si es reflexiva, simétrica y transitiva.

Por razones de simplificación se utiliza el símbolo $\sim$, y los elementos de todo par perteneciente a la relación se llaman equivalentes.

La notación $a \sim b$ se lee "$a$ es equivalente a $b$", y significa que el par $(a, b)$ pertenece a la relación. En este sentido, las relaciones de equivalencia satisfacen:

i ) **REFLEXIVIDAD.** Todo elemento de A es equivalnte a sí mismo.

$$\forall x : x \in A \Rightarrow x \sim x$$

ii ) **SIMETRIA.** Si un elemento es equivalente a otro, entonces éste es equivalente al primero.

$$\forall x \ \forall y : x \sim y \Rightarrow y \sim x$$

iii) **TRANSITIVIDAD.** Si un elemento es equivalente a otro, y éste es equivalente a un tercero, entonces el primero es equivalente al tercero.

$$\forall x \ \forall y \ \forall z : x \sim y \ \wedge \ y \sim z \Rightarrow x \sim z$$

***Ejemplo 3-10.***

En $A = \left\{ 1, 2, 3 \right\}$, la relación

$$\sim = \left\{ (1, 1), (2, 2), (3, 3), (1, 2), (2, 1) \right\}$$

es de equivalencia. Clasificamos las siguientes proposiciones:

| | | |
|---|---|---|
| $1 \sim 1$ V | $1 \sim 2$ V | $3 \sim 1$ F |
| $2 \sim 2$ V | $2 \sim 1$ V | $2 \sim 3$ F |
| $3 \sim 3$ V | $1 \sim 3$ F | $3 \sim 2$ F |

En virtud de las tres primeras queda asegurada la reflexividad. En cuanto a la simetría es suficiente ver que

$$1 \sim 2 \Rightarrow 2 \sim 1 \quad \text{es} \quad V$$

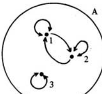
Más aun, si el antecedente es falso la implicación es verdadera

$$1 \sim 3 \Rightarrow 3 \sim 1$$

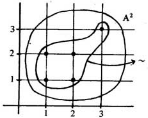
Para la transitividad, descartando los casos de antecedente falso, es suficiente verificar:

$$1 \sim 1 \ \wedge \ 1 \sim 2 \Rightarrow 1 \sim 2 \quad V$$
$$1 \sim 2 \ \wedge \ 2 \sim 1 \Rightarrow 1 \sim 1 \quad V$$
$$2 \sim 1 \ \wedge \ 1 \sim 2 \Rightarrow 2 \sim 2 \quad V$$
$$1 \sim 1 \ \wedge \ 1 \sim 1 \Rightarrow 1 \sim 1 \quad V$$

El diagrama de Venn es




donde cada arco orientado está asociado a un par perteneciente a la relación. En forma cartesiana:




### 3.8.2. Clases de equivalencia y conjunto cociente

Sea $\sim$ una relación de equivalencia en $A \neq \phi$. Un problema de interés es la determinación de todos los elementos de A que son equivalentes a uno dado, es decir, que forman pareja con él. La respuesta conduce en cada caso a un subconjunto de A, llamado clase de equivalencia del elemento.

***Definición***

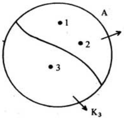
Clase de equivalencia del elemento $a \in A$ es el conjunto de todos los elementos de A equivalentes a $a$.

$$K_a = \left\{ x \in A \,/\, x \sim a \right\}$$

Con relación al ejemplo 3-10:

$$K_1 = \left\{ 1\,,\,2 \right\} = K_2$$
$$K_3 = \left\{ 3 \right\}$$

Es decir, hay dos clases de equivalencia, que son subconjuntos de A.



Podemos avanzar un poco más y preguntarnos por el conjunto cuyos elementos son las clases de equivalencia: $K_1$ y $K_3$.

Para denotarlo, podemos elegir un único elemento en cada clase de equivalencia, digamos 1 y 3, con lo que queda caracterizado un conjunto de índices $I = \{1, 3\}$,

de modo tal que a cada elemento de éste le está asociada una clase de equivalencia. El conjunto formado por las clases de equivalencia se llama conjunto cociente de A por la relación de equivalencia, y la notación es

$$\frac{A}{\sim} = \{ K_1, K_3 \}$$

o bien, mediante el conjunto de índices

$$\frac{A}{\sim} = \{ K_u \,/\, u \in I \}$$

Las clases de equivalencia constituyen una partición de A, en el sentido siguiente: son no vacías, disjuntas de a pares, y su unión es A. Este concepto será precisado en los párrafos siguientes, y es un hecho común a toda relación de equivalencia definida en un conjunto no vacío.

***Ejemplo 3-11.***

En el conjunto **Z** de los enteros introducimos la relación de congruencia módulo $n$, mediante la siguiente

***Definición***

Dos enteros son congruentes módulo $n$, si y sólo si $n$ es divisor de su diferencia. En símbolos

$$a \text{ y } b \text{ son congruentes módulo } n \Leftrightarrow n \mid a - b$$

Adelantándonos al hecho de que la congruencia es una relación de equivalencia podemos escribir

$$a \sim b \Leftrightarrow n \mid a - b \qquad (1)$$

Por definición, el número natural $n$ es divisor del entero $x$ si y sólo si éste es igual al primero por un entero, es decir

$$n \mid x \Leftrightarrow \exists\, k \in \mathbf{Z} \,/\, x = n \,.\, k$$

Especificamos las siguientes propiedades de la relación de divisor, que utilizaremos:

i ) Si un número divide a un entero, divide al producto de éste por cualquier entero.

$$n \mid x \Rightarrow n \mid x \,.\, y$$

En efecto, por definición de divisor

$$n \mid x \Rightarrow x = n \,.\, k \Rightarrow x \,.\, y = (n \,.\, k) \,.\, y \Rightarrow x \,.\, y = n \,.\, (k \,.\, y) \Rightarrow$$
$$\Rightarrow n \mid x \,.\, y$$

ii ) Si un número divide a otros dos, entonces divide a su suma o diferencia.

$$n \mid x \ \wedge \ n \mid y \Rightarrow n \mid x \pm y$$

Demostración)

Aplicando la definición de divisor a las dos proposiciones de la hipótesis, sumando y restando en **Z** aplicando la distributividad del producto respecto de la suma y resta, y la definición de divisor, tenemos

$$n \mid x \ \wedge \ n \mid y \Rightarrow x = n\,k \ \wedge \ y = n\,k' \Rightarrow$$
$$\Rightarrow x \pm y = n\,k \pm n\,k' \Rightarrow x \pm y = n\,(k \pm k') \Rightarrow$$
$$\Rightarrow n \mid x \pm y$$

iii) Si un número divide a un entero, entonces divide a su opuesto.

Es una consecuencia de la propiedad i ), ya que

$$n \mid x \Rightarrow n \mid (-1)\,.\,x \Rightarrow n \mid -x$$

Retomamos ahora nuestro propósito de probar que (1) es una relación de equivalencia.

a) Reflexividad.

Como $n \mid 0$, se tiene

$$\forall a : a \in \mathbf{Z} \Rightarrow n \mid a - a \Rightarrow a \sim a$$

b) Simetría. Sean los enteros $a$ y $b$ tales que

$$a \sim b \Rightarrow n \mid a - b \Rightarrow n \mid -(a-b) \Rightarrow n \mid b - a \Rightarrow b \sim a$$

por (1), propiedad iii), por opuesto de $a - b$ y por (1)

c) Transitividad. Sean los enteros $a$, $b$ y $c$, tales que

$$a \sim b \ \wedge \ b \sim c \Rightarrow n \mid a - b \ \wedge \ n \mid b - c \Rightarrow n \mid (a-b) + (b-c) \Rightarrow$$
$$\Rightarrow n \mid a - c \Rightarrow a \sim c$$

de acuerdo con (1), la propiedad ii ), reducción de términos, y (1).

Vamos a determinar las clases de equivalencia de los enteros. Sea $a \in \mathbf{Z}$; entonces:

$$K_a = \left\{ x \in \mathbf{Z} \,/\, x \sim a \right\}$$

Ahora traducimos la propiedad que define al conjunto $K_a$:

$$x \sim a \Rightarrow n \mid x - a \Rightarrow x - a = n\,.\,k \ \text{ con } \ k \in \mathbf{Z} \Rightarrow$$
$$\Rightarrow x = a + n\,.\,k \ \text{ con } \ k \in \mathbf{Z}$$

Es decir, a $K_a$ pertenecen todos los enteros del tipo $a + n\,.\,k$, donde $a$ y $n$ están dados, y $k$ recorre **Z**. En otras palabras, a $K_a$ pertenecen las sumas de $a$ con todos los

múltiplos de $n$. En particular:

$$K_0 = \{ \ldots\ldots, -2n, -n, 0, n, 2n, 3n, \ldots\ldots \}$$

$$K_1 = \{ \ldots\ldots, 1-2n, 1-n, 1, 1+n, 1+2n, 1+3n, \ldots\ldots \}$$

$$K_2 = \{ \ldots\ldots, 2-2n, 2-n, 2, 2+n, 2+3n, \ldots\ldots \}$$

................

$$K_{n-1} = \{ \ldots\ldots, -1-2n, -1-n, -1, -1+n, -1+2n, \ldots\ldots \}$$

Verificamos que no es posible obtener otras clases distintas de éstas; si queremos

$$K_n = \{ \ldots\ldots, -2n, -n, 0, n, 2n, 3n, \ldots\ldots \} = K_0$$

Análogamente: $K_{n+1} = K_1 = K_{2n+1} = K_{1-n} =$ etc.

Los subíndices de las clases de equivalencia son los posibles restos de la división de un entero por $n$, es decir: $0, 1, 2, \ldots, n-1$, ya que de acuerdo con el algoritmo de la división entera el resto es no negativo y menor que el divisor. Por este motivo reciben el nombre de clases de restos módulo $n$, y suelen denotarse mediante

$$\overline{0}, \overline{1}, \overline{2}, \ldots\ldots, \overline{n-1}$$

El conjunto cociente es

$$\frac{\mathbf{Z}}{\sim} = \{ \overline{0}, \overline{1}, \overline{2}, \ldots\ldots, \overline{n-1} \} = \mathbf{Z}_n$$

O bien

$$\mathbf{Z}_n = \{ K_u \,/\, 0 \leqslant u < n \}$$

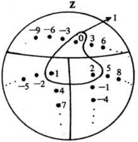
Lo mismo que en el ejemplo 3-10, las $n$ clases de equivalencia son no vacías, disjuntas dos a dos, y su unión es $\mathbf{Z}$.

Vamos a considerar el caso particular de las clases de restos módulo 3, en cuyo caso el conjunto cociente es

$$\mathbf{Z}_3 = \{ \overline{0}, \overline{1}, \overline{2} \} = \{ K_0, K_1, K_2 \}$$

donde $\overline{0}$ es el conjunto de todos los múltiplos de 3, o lo que es lo mismo, el conjunto de los enteros que divididos por 3 dan resto nulo; a $\overline{1}$ pertenecen los enteros que divididos por 3 dan resto 1, y análogamente $\overline{2}$.

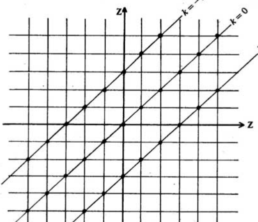
La partición de $\mathbf{Z}$ es




Realizamos la representación cartesiana de la relación. De acuerdo con (1), se trata del subconjunto de $\mathbf{Z}^2$ cuyos elementos son los pares ordenados de enteros $(x, y)$, que satisfacen

$$3 \mid x - y \Rightarrow x - y = 3\,k \text{ con } k \in \mathbf{Z} \Rightarrow y = x - 3\,k \text{ con } k \in \mathbf{Z}$$

Para cada entero $k$ quedan determinados los puntos de coordenadas enteras de la recta $y = x - 3\,k$, y en consecuencia, la relación consiste en el siguiente conjunto discreto de puntos del plano



$$k = 0 \Rightarrow y = x$$
$$k = -1 \Rightarrow y = x + 3$$
$$k = 1 \Rightarrow y = x - 3$$
$$k = 2 \Rightarrow y = x - 6 \text{, etc.}$$

La relación es

$$R = \bigcup_{k \in \mathbf{Z}} \left\{ (x, y) \in \mathbf{Z}^2 \,/\, y = x - 3k \right\}$$

### 3.8.3. Partición de un conjunto no vacío

Sean dos conjuntos $A \neq \phi$ e $I \neq \phi$ tales que, cualquiera que sea el elemento $u \in I$, existe un subconjunto $K_u \subset A$.

***Definición***

El conjunto $\left\{ K_u \,/\, u \in I \right\}$ es una partición de A si y sólo si

i ) $\forall u : u \in I \Rightarrow K_u \neq \phi$

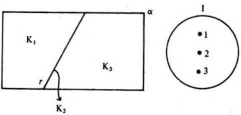
ii ) $u \neq v \Rightarrow K_u \cap K_v = \phi$

iii) $\forall a \in A \,,\, \exists u \in I \,/\, a \in K_u$

Los elementos $K_u$ de la partición son subconjuntos no vacíos de A, y están asociados al conjunto de índices I; además, elementos distintos del conjunto de índices determinan subconjuntos disjuntos de A; finalmente, la condición iii) significa que la unión de los subconjuntos de A que son elementos de la participación, es A.

***Ejemplo 3-12.***

i ) Sea $r$ una recta contenida en el plano $\alpha$. El plano queda particionado en tres subconjuntos $K_1$, $K_2$, $K_3$, siendo $I = \left\{ 1, 2, 3 \right\}$ un conjunto de índices.




ii ) Las relaciones de equivalencia de los ejemplos 3-10 y 3-11 conducen a las particiones indicadas en éstos.

iii) Investigamos la partición asociada a la relación de equivalencia del ejemplo 3-8. En este caso, la relación está definida en R mediante

$$a \sim b \Leftrightarrow a - b \in \mathbf{Z}$$

Sea $a \in \mathbf{R}$; entonces, por definición de clase de equivalencia

$$K_a = \left\{ x \in \mathbf{R} \,/\, x \sim a \right\}$$

Ahora bien

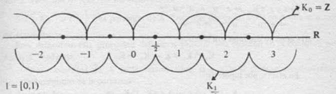
$$x \sim a \Rightarrow x - a \in \mathbf{Z} \Rightarrow x - a = k \text{ con } k \in \mathbf{Z}$$

Entonces a $K_a$ pertenecen todos los reales del tipo

$$x = a + k \quad \text{siendo} \quad k \in \mathbf{Z}$$

Es decir, todos los elementos equivalentes a $a$, se obtienen sumando a $a$ todos los enteros. En consecuencia, si elegimos como conjunto de índices al intervalo semiabierto $I = [0\,,\,1)$, la partición R es

$$\frac{\mathbf{R}}{\sim} = \left\{ K_u \,/\, u \in [0,1) \right\}$$




### 3.8.4. Teorema fundamental de las relaciones de equivalencia definidas en un conjunto no vacío

Vamos a demostrar lo que ya hemos verificado a través de ejemplos anteriores, a saber, que toda relación de equivalencia definida en un conjunto no vacío determina una partición de éste en clases de equivalencia.

TEOREMA

Si $\sim$ es una relación de equivalencia definida en el conjunto $A \neq \phi$, entonces existe un subconjunto $I \subset A$, tal que cualquiera que sea $u$ en I, existe $K_u \subset A$, de modo que se verifican las siguientes proposiciones:

i ) $u \in I \Rightarrow K_u \neq \phi$

ii ) $a \sim a' \Leftrightarrow a$ y $a'$ pertenecen al mismo $K_u$

iii) $K_u \cap K_v \neq \phi \Rightarrow K_u = K_v$

iv) $u \neq v \Rightarrow K_u \cap K_v = \phi$

v) $\forall a \in A, \exists u \in I / a \in K_u$

NOTA

I es un conjunto de índices que se forma eligiendo un único elemento en cada clase de equivalencia.

Demostración)

i) A todo elemento del conjunto de índices le corresponde una clase no vacía.

Por hipótesis, reflexividad y definición de clase de equivalencia:

$$A \neq \phi \Rightarrow \exists\, a \in A \Rightarrow a \sim a \Rightarrow a \in K_a \Rightarrow K_a \neq \phi\ \forall a \in A$$

Ahora bien, como $I \subset A$

$$u \in I \Rightarrow u \in A \Rightarrow K_u \neq \phi$$

ii) Dos elementos de A son equivalentes si y sólo si pertenecen a la misma clase.

a) $a \sim a' \Rightarrow a' \in K_a \ \wedge\ a \in K_a$

Si $u \in K_a$ entonces $a$ y $a' \in K_u$

b) $a$ y $a' \in K_u \Rightarrow a \sim u \ \wedge\ a' \sim u \Rightarrow$

$\Rightarrow a \sim u \ \wedge\ u \sim a' \Rightarrow a \sim a'$

iii) Clases no disjuntas son idénticas.

$$K_u \cap K_v \neq \phi \Rightarrow K_u = K_v$$

En efecto, por hipótesis:

$$K_u \cap K_v \neq \phi \Rightarrow \exists\, x \in K_u \cap K_v \Rightarrow$$
$$\Rightarrow \exists\, x \in A / x \in K_u \ \wedge\ x \in K_v \Rightarrow$$
$$\Rightarrow x \sim u \ \wedge\ x \sim v \Rightarrow u \sim x \ \wedge\ x \sim v \qquad (1)$$

Sea

$$y \in K_u \Rightarrow y \sim u \qquad (2)$$

De (1) y (2), por transitividad

$$y \in K_u \Rightarrow y \sim v \Rightarrow y \in K_v$$

O sea $K_u \subset K_v$

Análogamente $K_v \subset K_u$, y resulta

$$K_u = K_v$$

iv) Elementos distintos del conjunto de índices determinan clases disjuntas.

$u \neq v \Rightarrow K_u \cap K_v = \phi$

Suponemos $K_u \cap K_v \neq \phi \Rightarrow \exists\, x \in K_u \;\wedge\; x \in K_v \Rightarrow$

$\Rightarrow x \sim u \;\wedge\; x \sim v \Rightarrow \; u \sim x \;\wedge\; x \sim v \Rightarrow$

$\Rightarrow u \sim v \Rightarrow u \in K_v$. Absurdo porque contradice la definición de I.

v ) Todo elemento de A pertenece a una clase, o lo que es lo mismo, las clases de equivalencia "cubren" a A.

Sea $a \in A \Rightarrow a \sim a \Rightarrow a \in K_a$ (1)

Si $u \in K_a$, entonces $K_a = K_u$, y resulta $a \in K_u$.

NOTA

Las proposiciones i ), iv) y v ) significan que toda relación de equivalencia, definida en conjunto no vacío, determina una partición de éste en clases de equivalencia. Precisamente, las clases son los elementos de la partición.

### 3.8.5. Partición y relación de equivalencia

Sea $\left\{ K_u \,/\, u \in I \right\}$ una partición de A. Entonces queda inducida en A una relación de equivalencia.

Para demostrar esta propiedad definimos primero una relación en el conjunto no vacío A, mediante

"dos elementos de A están relacionados, si y sólo si pertenecen al mismo subconjunto de la partición".

En símbolos

$$(a\,,\,b) \in R \Leftrightarrow a \text{ y } b \text{ pertenecen al mismo } K_u \qquad (1)$$

Vamos a probar que es de equivalencia.

i ) Reflexividad.

Por definición de partición

$$a \in A \Rightarrow \exists\, u \in I \,/\, a \in K_u \Rightarrow a \text{ y } a \text{ pertenecen a } K_u$$

Entonces, por (1) $(a\,,\,a) \in R$

ii ) Simetría. Sean $a$ y $b$ en A, tales que

$$(a\,,\,b) \in R \Rightarrow a \text{ y } b \text{ pertenecen al mismo } K_u \Rightarrow$$

$$\Rightarrow b \text{ y } a \text{ pertenecen al mismo } K_u \Rightarrow (b\,,\,a) \in R$$

iii) Transitividad. Sean $a$ , $b$ y $c$ en A, tales que

$(a , b) \in R \;\wedge\; (b , c) \in R \Rightarrow a , b$ y $c$ pertenecen al mismo $K_u \Rightarrow$

$\Rightarrow a$ y $c$ pertenecen al mismo $K_u \Rightarrow (a , c) \in R$

*Ejemplo 3-13.*

Se considera en $A = \left\{ 1 , 2 , 3 \right\}$ la siguiente partición:

$$\left\{ \left\{ 1 , 3 \right\} , \left\{ 2 \right\} \right\}$$

La relación de equivalencia correspondiente es, entonces

$$\left\{ (1 , 1) , (3 , 3) , (1 , 3) , (3 , 1) , (2 , 2) \right\}$$

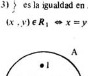
De acuerdo con 3.8.4 y 3.8.5, los conceptos de partición y de relación de equivalencia son identificables. Es claro que en un conjunto no vacío es posible definir tantas relaciones de equivalencia como particiones.

A continuación proponemos todas las relaciones de equivalencia definibles en el conjunto A.

a)

$R_1 = \left\{ (1 , 1) , (2 , 2) , (3 , 3) \right\}$ es la igualdad en A, es decir

$$(x , y) \in R_1 \Leftrightarrow x = y$$

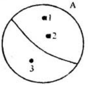



b)

$R_2 = \left\{ (1 , 1) , (2 , 2) , (1 , 2) , (2 , 1) , (3 , 3) \right\}$

**En este caso**

$$(x\,,y)\in R_2 \Leftrightarrow x=y \;\vee\; x+y=3$$

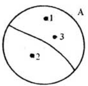



c)

$R_3 = \left\{ (1\,,1)\,,(3\,,3)\,,(1\,,3)\,,(3\,,1)\,,(2\,,2) \right\}$

O sea

$$(x\,,y)\in R_3 \Leftrightarrow x=y \;\vee\; x+y=4$$

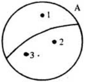



d)

$R_4 = \left\{ (1\,,1)\,,(2\,,2)\,,(3\,,3)\,,(2\,,3)\,,(3\,,2) \right\}$

Siendo

$$(x\,,y)\in R_4 \Leftrightarrow x=y \;\vee\; x+y=5$$

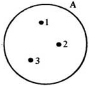


e)

$$R_5 = \left\{(1,1), (2,2), (3,3), (1,2), (2,1), (1,3), (3,1), (2,3), (3,2)\right\} = A^2$$

Es decir

$$(x, y) \in R_5 \Leftrightarrow (x, y) \in A^2$$




Aquí la partición consiste en un único subconjunto: el mismo A.

## 3.9. RELACIONES DE ORDEN

Es usual en matemática y en la vida cotidiana ordenar los elementos de un conjunto de acuerdo con algún criterio conveniente. El orden queda especificado a través del término "preceder", y decir

"$x$ precede a $y$" significa $(x, y) \in R$

Lo esencial de toda relación de orden es la transitividad, y según se cumplan o no otras propiedades se habla de orden amplio o estricto, y en cada caso, de orden parcial o total.

### 3.9.1. Orden amplio

Sea $R \subset A^2$.

*Definición*

$R$ es una relación de orden amplio en A si y sólo si es reflexiva, antisimétrica y transitiva.

Obviando los cuantificadores universales tenemos:

i ) Reflexividad.

$$a \in A \Rightarrow (a, a) \in R$$

ii ) Antisimetría.

$$(a,b) \in R \ \wedge \ (b,a) \in R \Rightarrow a = b$$

iii) Transitividad.

$$(a,b) \in R \ \wedge \ (b,c) \in R \Rightarrow (a,c) \in R$$

### 3.9.2. Orden parcial y total

Sea $R$ una relación de orden en A.

i ) $R$ es de orden parcial si y sólo si existen pares de elementos incomparables, es decir

$$\exists a \,,\, \exists b \,/\, (a,b) \notin R \ \wedge \ (b,a) \notin R$$

ii ) El orden es total en caso contrario, es decir

$$a \neq b \Rightarrow (a,b) \in R \ \vee \ (b,a) \in R$$

**Ejemplo 3-14**

i ) En N la relación de divisor es de orden amplio y parcial.

Por definición

$$n \mid a \Leftrightarrow \exists\, m \in \mathbf{N} \,/\, a = n \,.\, m$$

a) Reflexividad.

$$a \in \mathbf{N} \Rightarrow a = a \,.\, 1 \Rightarrow a | a$$

b) Antisimetría.

Sean $a \mid b \ \wedge \ b \mid a \Rightarrow \quad n$ y $m$ en $\mathbf{N} \,/\, b = a \,.\, n \ \wedge \ a = b \,.\, m \Rightarrow$

$\Rightarrow a \,.\, b = a \,.\, n \,.\, b \,.\, m \Rightarrow 1 = n \,.\, m \Rightarrow n = m = 1$

Luego $a = b$.

c) Transitividad.

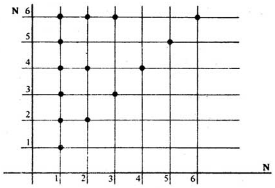
Sean $\quad a \mid b \ \wedge \ b \mid c \Rightarrow b = a \,.\, n \ \wedge \ c = b \,.\, m$

Entonces $\ b \,.\, c = a \,.\, n \,.\, b \,.\, m \Rightarrow c = a \,.\, (n \,.\, m) \Rightarrow c = a \,.\, p \Rightarrow a \mid c$.

Por otra parte, este orden amplio es parcial, pues existen pares de naturales que no son comparables por la relación de divisor. Un contraejemplo está dado por 2 y 3, ya que $2|3$ y $3|2$ son proposiciones falsas.

Es claro que un par ordenado de números naturales pertenece a la relación si y sólo si la primera componente es divisor de la segunda.

Esta relación está representada por los puntos del primer cuadrante de coordenadas naturales que tienen abscisa natural, y para cada una las ordenadas son todos los múltiplos naturales de aquéllas.




Si consideramos la relación de divisor en Z, no se tiene un orden amplio, pues la antisimetría no se cumple. En efecto

$$3 \mid -3 \ \wedge \ -3 \mid 3 \Rightarrow 3 = -3 \quad \text{es F}$$

ii ) En $A = \{1, 2, 3\}$ la relación

$R = \{(1,1), (2,2), (3,3), (1,2), (1,3), (2,3)\}$ es un orden amplio y total. Se trata evidentemente de la relación de menor o igual.

### 3.9.3. Orden estricto.

Sea $R \subset A^2$

***Definición***

$R$ es una relación de orden estricto si y sólo si es arreflexiva, asimétrica y transitiva.

En símbolos

i ) Arreflexividad. Ningún elemento del conjunto está relacionado consigo mismo.

$$a \in A \Rightarrow (a, a) \notin R$$

ii ) Asimetría. Si un elemento está relacionado con otro, entonces éste no lo está con el primero.

$$(a, b) \in R \Rightarrow (b, a) \notin R$$

iii) Transitividad.

$$(a,b)\in R \ \wedge \ (b,c)\in R \Rightarrow (a,c)\in R$$

Lo mismo que el orden amplio, el orden estricto puede ser parcial o total.

*Ejemplo 3-15.*

i ) La relación de menor en R es un orden estricto y total.

ii ) Por definición, un conjunto está estrictamente incluido en otro si y sólo si todo elemento del primero pertenece al segundo, pero existen elementos de éste que no pertenecen al primero. La notación y símbolos son los siguientes:

$$A \subsetneqq B \Leftrightarrow A \subset B \ \wedge \ A \neq B$$

En $P(U)$ la inclusión estricta es una relación de orden estricto y parcial, como puede verificarse sencillamente.

iii) En $A = \{a, b, c\}$ la relación

$R = \{(a,b), (a,c), (b,c)\}$ es de orden estricto y total.

### 3.9.4. El signo de preceder

Si $R$ es una relación de orden definida en A, y dos elementos $a$ y $b$ están vinculados por dicha relación, al escribir $(a,b)\in R \ \vee \ a\,R\,b$ suele decirse que "$a$ precede a $b$", y la notación es $a \prec b$.

Con esta notación se tiene:

i ) Reflexividad.

$$a \in A \Rightarrow a \prec a$$

ii ) Antisimetría.

$$a \prec b \ \wedge \ b \prec a \Rightarrow a = b$$

iii) Transitividad.

$$a \prec b \ \wedge \ b \prec c \Rightarrow a \prec c$$

iv) Linealidad.

$$a \neq b \Rightarrow a \prec b \ \underline{\vee} \ b \prec a$$

Análogamente, para la arreflexividad, asimetría, orden parcial y total, teniendo en cuenta que "$a$ no precede a $b$" puede escribirse $a \not\prec b$.

### 3.9.5. Elementos distinguidos de un conjunto ordenado

Sea A un conjunto ordenado por una relación de orden $\prec$.

i ) *Primer elemento.* El elemento $a \in A$ se llama primer elemento si y sólo si precede a todos los demás.

$$a \in A \text{ es el primer elemento } \Leftrightarrow \quad \in A \Rightarrow a \prec x$$

ii ) *Ultimo elemento.* El elemento $b \in A$ se llama último elemento si y sólo si todo elemento de A precede a $b$.

$$b \in A \text{ es el último elemento } \Leftrightarrow x \in A \Rightarrow x \prec b$$

De estas definiciones no se deduce que todo conjunto ordenado deba tener necesariamente primero o último elemento; puede ocurrir que carezca de .mbos, que tenga primero o bien último, o que tenga primero y último.

iii) *Elementos minimales.* El objeto $m$ de A es un elemento minimal si y sólo si no existe un elemento distinto que lo preceda.

$$m \in A \text{ es minimal } \Leftrightarrow \forall x \in A: \quad \prec \quad \Rightarrow m = x$$

iv) *Elementos maximales.* El objeto $n$ es un elemento maximal si y sólo si no existe en A un elemento distinto que lo siga.

$$n \in A \text{ es maximal } \Leftrightarrow \forall x \in A: \quad \prec \quad \Rightarrow x = n$$

Puede ocurrir que en un conjunto ordenado no existan elementos minimales o maximales, y si existen pueden no ser únicos.

v ) *Cotas inferiores.* El elemento $a \in A$ es una cota inferior del subconjunto $X \subset A$ si y sólo si precede a todo elemento de X.

$$a \in A \text{ es cota inferior de } X \subset A \Leftrightarrow x \in X \Rightarrow a \prec x$$

vi ) *Cotas superiores.* El elemento $b \in A$ es una cota superior del subconjunto $X \subset A$ si y sólo si sigue a todo elemento de X.

$$b \in A \text{ es cota superior de } X \subset A \Leftrightarrow x \in X \Rightarrow x \prec b$$

vii) *Supremo o cota superior mínima.* El elemento $s \in A$ es el supremo del subconjunto $X \subset A$ si y sólo si es el primer elemento del conjunto de las cotas superiores.

viii) *Infimo o cota inferior máxima.* El elemento $i \in A$ es el ínfimo del subconjunto $X \subset A$ si y sólo si es el último elemento del conjunto de las cotas inferiores.

Las cotas de un conjunto, si existen, no son necesariamente únicas. En cambio, el ínfimo o supremo, aunque el conjunto no sea acotado, pueden no existir, ya que un conjunto ordenado puede carecer de primero o último elemento; pero si existen, son únicos. Precisamos los conceptos anteriores en los ejemplos siguientes.

***Ejemplo 3-16.***

i ) Consideramos el intervalo abierto $(-1\ ,\ 1) \subset \mathbf{R}$, donde se define la relación de menor o igual.

Esta relación en **R** es de orden amplio y total, pues

a) Reflexividad.

$$a \in \mathbf{R} \Rightarrow a \leqslant a$$

b) Antisimetría.

$$a \leqslant b \ \wedge \ b \leqslant a \Rightarrow a = b$$

c) Transitividad.

$$a \leqslant b \ \wedge \ b \leqslant c \Rightarrow a \leqslant c$$

d) Linealidad.

$$a \neq b \Rightarrow a \leqslant b \ \vee \ b \leqslant a$$

No existen en $(-1, 1)$ ni primero ni último elemento, ya que los extremos $-1$ y 1 no pertenecen al intervalo abierto. Tampoco existen elementos minimales ni maximales. Es claro que cotas inferiores de $(-1, 1)$ hay infinitas: todos los reales menores o iguales que $-1$. Análogamente son cotas superiores todos los números reales mayores o iguales que 1. El ínfimo es $-1$ y el supremo es 1, y ninguno pertenece al conjunto $(-1, 1)$.

ii) Con la misma relación de menor o igual el intervalo semiabierto $[-1, 1)$ tiene primer elemento $-1$, que es también minimal, cota inferior e ínfimo. Carece de último elemento, de elementos maximales, de cotas superiores y de supremo.

iii) Sea ahora el conjunto $A = \left\{ 2, 3, 6, 9, 12, 36 \right\}$ ordenado por la relación de divisibilidad. Se ha visto que el orden es amplio y parcial. Como no existe en A ningún elemento que sea divisor de todos los demás carece de primer elemento, pero tiene último y es 36. Este es elemento maximal, y tanto 2 como 3, son minimales. No hay cotas inferiores ni ínfimo, pero la cota superior y el supremo son 36.

### 3.9.6. Diagramas de Hasse

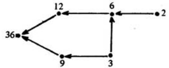
Sea A un conjunto ordenado.

i) *Elementos consecutivos.* Los elementos $a$ y $b$ de A son consecutivos si y sólo si

a) $a < b$
b) $a < x < b \Rightarrow a = x \ \vee \ b = x$

ii) *Representación de conjuntos ordenados.* Es posible representar un conjunto ordenado y finito, mediante un diagrama llamado de Hasse, asignando a cada elemento del conjunto un punto del plano o bien del espacio, y uniendo cada par de elementos consecutivos por medio de un vector orientado en el sentido de $x$ a $y$, si $x < y$.

Así, el diagrama de Hasse correspondiente al conjunto $A = \{2, 3, 6, 9, 12, 36\}$, ordenado por la relación de divisor, es




Toda poligonal orientada determina un subconjunto totalmente ordenado por la misma relación, y constituye una cadena.

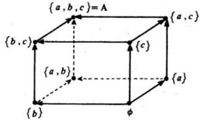
***Ejemplo 3-17.***

Dado $A = \{a, b, c\}$, en $P(A)$ consideramos la relación de inclusión, definida por

$$X < Y \Leftrightarrow X \subset Y$$

De acuerdo con 2.3.4., esta relación es de orden amplio y parcial en $P(A)$.

El correspondiente diagrama de Hasse es la siguiente representación espacial




El conjunto $P(A)$ tiene primer elemento y último elemento: $\phi$ y A, respectivamente. Ambos son el elemento minimal y maximal. A dos elementos cualesquiera de $P(A)$ les corresponde una cota inferior máxima y una cota superior mínima, es decir, un ínfimo y un supremo. Así, dados $\{a, b\}$ y $\{a, c\}$ el ínfimo es $\{c\}$ y el supremo es $\{a, b, c\}$. Cuando esto ocurre para todo par de elementos de un conjunto ordenado, se dice que el conjunto tiene una estructura de red o de reticulado, o de lattice.

### 3.9.7. Conjuntos bien ordenados

Sea $<$ una relación de orden en A.

***Definición***

Un conjunto está bien ordenado por una relación de orden si y sólo si está totalmente ordenado, y además todo subconjunto no vacío tiene primer elemento.

*Ejemplo 3-18.*

i ) El conjunto de los números reales, ordenado por la relación de "menor o igual", está totalmente ordenado, pero no es un conjunto bien ordenado, pues no todo subconjunto no vacío de **R** tiene primer elemento. En efecto, el intervalo abierto $(-1, 1)$ es una parte no vacía de **R**, pero carece de primer elemento.

ii ) El conjunto **Z** de los enteros está totalmente ordenado por la misma relación, pero como carece de primer elemento no está bien ordenado.

iii) El conjunto **N** de los números naturales está bien ordenado por la relación de menor o igual, ya que se halla totalmente ordenado, y toda parte no vacía de **N** tiene primer elemento.

iv) El conjunto cuyos elementos son $\phi$, $\{a\}$, $\{a, b\}$, $\{a, b, c\}$ está bien ordenado por la relación de inclusión.

v ) El conjunto $A = \{2, 3, 6, 9, 12, 36\}$ propuesto en 3.9.6. ii ), ordenado por la relación de divisor, no está bien ordenado, por no ser totalmente ordenado.

## TRABAJO PRACTICO III

*3-19.* Sean $A=\{x \in \mathbf{N} / 1 \leqslant x \leqslant 5\}$ y $B=\{3, 4, 5\}$

Se define $R \subset A \times B$ mediante

$$(x, y) \in R \Leftrightarrow x+y \lesssim 5$$

i ) Definir $R$ por extensión.

ii ) Representar $A \times B$ y $R$.

iii) Determinar $R^{-1}$.

*3-20.* Se consideran $A=\{1, 2, 3, 4, 5\}$ $B=\{1, 4, 6, 16\}$ $C=\{2, 3, 8, 10\}$ y las relaciones $R \subset A \times B$, $S \subset B \times C$, definidas por

$$(x, y) \in R \Leftrightarrow y=x^2$$

$$(y, z) \in S \Leftrightarrow z=\frac{y}{2}$$

Se pide:

i ) Determinar $R$ y $S$ por extensión.

ii ) Definir la composición $S \circ R \subset A \times C$ por extensión.

iii) Determinar los dominios e imágenes de las tres relaciones.

*3-21.* Obtener los gráficos cartesianos de las siguientes relaciones definidas en **R**:

i ) $(x, y) \in R \Leftrightarrow y=3$

ii ) $(x, y) \in S \Leftrightarrow x+y=1$

iii) $(x, y) \in T \Leftrightarrow x+y<1$

*3-22.* En **Z** se define $R$ mediante

$$(a, b) \in R \Leftrightarrow a^2+a=b^2+b$$

Clasificar $R$.

*3-23.* En $\mathbf{R}^2$ se define la relación "$\sim$" mediante

$$(x, y) \sim (x', y') \Leftrightarrow y=y'$$

Probar que es de equivalencia, determinar las clases de equivalencia, un conjunto de índices y el conjunto cociente.

*3-24.* En $A=\{1, 2, 4, 6, 8\}$ se define la siguiente relación

$$(x, y) \in R \Leftrightarrow 3 \mid x+y$$

i ) Definir a $R$ por extensión.

ii ) Formar el diagrama de $R$.

iii) Clasificar $R$.

**3-25.** En $\mathbf{N}^2$ se considera la siguiente relación

$$(a, b) \sim (a', b') \Leftrightarrow a + b' = b + a'$$

Demostrar que es de equivalencia, obtener las clases de equivalencia, un conjunto de índices, el conjunto cociente, y representar las clases.

**3-26.** El conjunto $\left\{\left\{a\right\}, \left\{b, c\right\}, \left\{d\right\}\right\}$ es una partición de $A = \left\{a, b, c, d\right\}$. Obtener la relación de equivalencia asociada.

**3-27.** En $A = \left\{1, 2, 3, 4\right\}$ se considera la relación

$$R = \left\{(x, y) \in A^2 \ / \ x = y \ \vee \ x + y = 3\right\}$$

Definir $R$ por extensión, probar que es de equivalenvia y determinar la correspondiente partición de A.

**3-28.** Clasificar la relación $R$ definida en $\mathbf{Z}^2$ mediante

$$(a, b) \, R \, (a', b') \Leftrightarrow ab' = ba'$$

**3-29.** En el conjunto de los números reales se define

$$R = \left\{(x, y) \in \mathbf{R}^2 \ / \ |x - 1| = |y - 1|\right\}$$

Demostrar que es de equivalencia, y representarla.

**3-30.** Una relación $R$ definida en un conjunto A es circular si y sólo si

$$(a, b) \in R \ \wedge \ (b, c) \in R \Rightarrow (c, a) \in R$$

Demostrar que una relación es reflexiva y circular si y sólo si es de equivalencia.

**3-31.** En $\mathbf{R}$ se define "$\sim$" mediante

$$x \sim y \Leftrightarrow x^2 - x = y^2 - y$$

Demostrar que es de equivalencia, determinar las clases, un conjunto de índices, el cociente, y representar la relación.

**3-32.** Sean $R$ y $S$ dos relaciones definidas en A. Demostrar:
Si $R$ y $S$ son reflexivas, entonces $R \cup S$ y $R \cap S$ son reflexivas.

**3-33.** En $\mathbf{R}$ se define

$$R = \left\{(x, y) \in \mathbf{R}^2 \ / \ |x| + 2\,|y| = 1\right\}$$

Obtener el dominio, la imagen y el gráfico cartesiano de $R$.

**3-34.** Sea $R \subset A^2$. Demostrar que la relación $R \cup R^{-1}$ es simétrica.

**3-35.** Clasificar y representar la relación $R \subset \mathbf{R}^2$ definida por

$$(x, y) \in R \Leftrightarrow x - y \in \mathbf{R}^+$$

*3-36.* En $A = [-1, 1]$ se considera la relación

$$R = \left\{ (x, y) \in A^2 / x^2 = y^2 \right\}$$

i ) Representar $R$.

ii ) Probar que es de equivalencia.

iii) Obtener la partición de A.

*3-37.* Sea $R$ una relación definida en A.
Demostrar:

i ) $R$ es simétrica $\Rightarrow R^{-1}$ es simétrica.

ii) $R$ es transitiva $\Rightarrow R^{-1}$ es transitiva.

*3-38.* Sean $R$ y $R'$ dos relaciones transitivas en A.
Demostrar que $R \cap R'$ es transitiva.

*3-39.* Si $R$ y $R'$ son dos relaciones antisimétricas en A, entonces $R \cap R'$ es antisimétrica.

*3-40.* Sean "$\sim$" una relación de equivalencia definida en $A \neq \phi$ y $X \subset A$. Por definición, se llama saturado de X por la relación de equivalencia al conjunto de los elementos de A que son equivalentes a los elementos de X.
La notación es:

$$X^* = \left\{ x \in A / x \sim y , \forall y \in X \right\}$$

Demostrar:

i ) $X \subset X^*$

ii ) $(X \cup Y)^* = X^* \cup Y^*$

*3-41.* Clasificar las siguientes relaciones definidas en el conjunto de las rectas del plano

i ) $(a, b) \in R \Leftrightarrow a \cap b \neq \phi$

ii ) $(a, b) \in R \Leftrightarrow a \perp b$

3-42. Clasificar todas las relaciones del ejemplo 3-3.

*3-43.* Clasificar la relación $R$ definida en **R** mediante

$$(x, y) \in R \Leftrightarrow |x + y| = 2$$

*3-44.* En $A = \left\{ 1, 2, 3, 4, 5 \right\}$ se considera la relación de menor o igual.
Determinar los elementos maximales y minimales.

*3-45.* Definir por extensión la relación de divisor en el conjunto del ejercicio 3-44, y obtener los elementos maximales y minimales.

*3-46.* Con relación al ejercicio 3-45, determinar una cota superior y una inferior del subconjunto $\left\{ 2, 3 \right\}$

**3-47.** En **R**, ordenado por la relación de menor o igual, se considera

$$A=\left\{x\in \mathbf{R}\,/\,x=\frac{1}{n}\quad\wedge\ n\in \mathbf{N}\right\}$$

Investigar si A tiene primero o último elemento, si está bien ordenado, y si admite cotas, ínfimo o supremo.

Capítulo 4

# *FUNCIONES*

## 4.1. INTRODUCCION

Dada la importancia del tema a desarrollar hemos preferido asignarle un capítulo especial, con abundante ejercitación y ejemplos. Por otra parte, en virtud del carácter elemental del texto, y la conveniencia de que en primera instancia el concepto sea utilizado con dinamismo y seguridad, se ha prescindido del estudio de las correspondencias. Se estudian las funciones o aplicaciones especiales, la composición de funciones, y el álgebra de las imágenes y preimágenes.

## 4.2. RELACIONES FUNCIONALES

Sean A y B dos conjuntos no vacíos, que llamaremos dominio y codominio respectivamente. Entenderemos por función de A en B toda regla que hace corresponder a cada elemento del dominio un único elemento del codominio. Más precisamente, una función es un conjunto de pares ordenados tales que la primera componente pertenece a A y la segunda a B, es decir, un subconjunto de $A \times B$, de modo que todo elemento de A sea primera componente de un par y sólo de uno. Esto nos dice que toda función de A en B es una relación especial entre A y B.

Usualmente, los signos que indican funciones son $f$, $g$, $h$, etcétera. Así, para denotar que $f$ es una función de A en B, se escribe:

$$f : A \rightarrow B$$

y se lee: "$f$ es una función o aplicación de A en B", o bien "$f$ es una función con dominio A y codominio B".

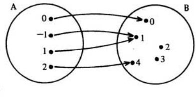
En particular, si $A = \{-1, 0, 1, 2\}$, $B = \{0, 1, 2, 3, 4\}$ y $f$ es la relación definida por

$$(x, y) \in f \Leftrightarrow y = x^2$$

entonces se tiene

$f = \{ (-1, 1), (0, 0), (1, 1), (2, 4) \}$ ya que cada segunda componente es el cuadrado de la primera.

El diagrama de Venn correspondiente es




Tanto en la definición de $f$ por extensión como en el diagrama es fácil advertir que todo elemento del dominio tiene un correspondiente o imagen en el codominio; y además tal correspondiente es único, en el sentido de que no se tienen dos pares ordenados distintos con la misma primera componente. Resulta entonces que $f$ es una función de A en B. Observamos aquí las siguientes situaciones: elementos distintos de A pueden tener la misma imagen en B, como ocurre con $-1$ y $1$, cuyas imágenes son 1; además, puede darse que elementos de B no tengan un antecedente en A, es decir, que pueden existir en B elementos que no sean correspondientes de ningún elemento de A, como ocurre con 2 y 3.

***Definición***

$f$ es una función o aplicación de A en B si y sólo si $f$ es una relación entre A y B, tal que todo elemento de A tiene un único correspondiente en B.

O bien:

***Definición***

$f$ es una función o aplicación de A en B si y sólo si $f$ es un subconjunto de $A \times B$ que satisface las siguientes condiciones de existencia y unicidad:

i ) $\forall a \in A, \exists b \in B / (a, b) \in f$

ii ) $(a, b) \in f \wedge (a, c) \in f \Rightarrow b = c$

Si $(a, b) \in f$ decimos que $b$ es el correspondiente o imagen de $a$, por $f$, y suele escribirse $b = f(a)$, es decir, $b$ es el trasformado de $a$ por la función $f$.

Para denotar la misma cosa, algunos autores utilizan la notación a izquierda:

$$af = b$$

Una función queda especificada si se dan el dominio A, el codominio B, y además la relación $f \subset A \times B$, que satisface las condiciones i ) y ii ) de la definición.

Por ser un conjunto, $f$ puede estar dado por extensión, es decir, como conjunto de pares ordenados, o bien por comprensión, mediante una fórmula o ley de correspondencia-que permita asignar a cada objeto del dominio su imagen en el codominio.

***Ejemplo 4-1.***

Determinamos si las siguientes relaciones son funciones.

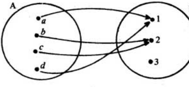
i ) Sean $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$ y la relación

$$f = \{(a, 1), (b, 2), (c, 2), (d, 1)\}$$

Se cumplen las condiciones de la definición, y resulta $f$ una función tal que

$$f(a) = 1 \qquad f(b) = 2 \qquad f(c) = 2 \qquad f(d) = 1$$

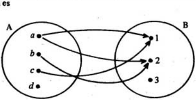
El diagrama es




ii ) Con los mismos A y B, la relación

$$\{(a, 1), (a, 2), (b, 2), (c, 1)\}$$

no es una función por las siguientes razones: no se cumple i ), ya que no todo elemento del dominio A tiene imagen en el codominio B, pues $d$ carece de trasformado. También deja de verificarse ii ), puesto que un mismo elemento de A tiene dos imágenes en B, como ocurre con $a$. El diagrama de la relación es



iii) Si A es el conjunto de las personas y $f$ es la relación en A definida por

$$(x, y) \in f \Leftrightarrow x \text{ es hijo de } y$$

entonces $f$ es una función de A en A, ya que toda persona tiene padre y éste es único.

En cambio la relación definida en el mismo A mediante

$$(x, y) \in f \Leftrightarrow x \text{ es padre de } y$$

no es una función de A en A, ya que existen en A personas que no son padres, es decir, elementos del dominio que carecen de imagen en el codominio; por otra parte, tampoco se verifica la unicidad, pues existen personas que son padres de más de un hijo. Esto significa que si una relación es función, la relación inversa no lo es necesariamente.

## 4.3. REPRESENTACION CARTESIANA DE FUNCIONES

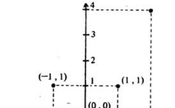
Lo mismo que las relaciones, las funciones pueden representarse mediante un sistema de coordenadas cartesianas en el plano o en el espacio, según que el dominio sea unidimensional o bidimensional, respectivamente. En el caso de representaciones planas, el dominio es un subconjunto del eje horizontal, y el codominio, del eje vertical.

*Ejemplo 4-2.*

Representación cartesiana de la función propuesta en 4.2.

$$A = \{-1, 0, 1, 2\} \quad B = \{0, 1, 2, 3, 4\}$$

$$f(x) = y = x^2$$



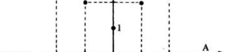
***Ejemplo 4-3.***

Sean $A = \{-2, -1, 0, 1, 2\}$, $B = \mathbf{N}$ y $f: A \to \mathbf{N}$ tal que

$$f(x) = |x| + 1$$

resulta $f = \{(-2, 3), (-1, 2), (0, 1), (1, 2), (2, 3)\}$

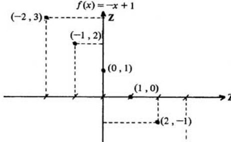
Cada elemento $(a, b) \in f$ es un punto del plano de coordenadas $a$ y $b$. La representación cartesiana es




***Ejemplo 4-4.***

Sea $f: \mathbf{Z} \to \mathbf{Z}$ tal que la imagen de cada entero es su opuesto aumentado en 1, es decir

$$f(x) = -x + 1$$

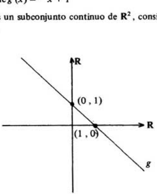


No es posible representar completamente a $f$, por ser $\mathbf{Z}$ un conjunto infinito; no obstante, la representación de algunos puntos nos sugiere el comportamiento de la aplicación. En éste, y en los ejemplos anteriores, el hecho de que cada elemento del dominio tenga una única imagen en el codominio se traduce en que a una misma abscisa le corresponde una sola ordenada.

*Ejemplo 4-5.*

Si $g : \mathbf{R} \to \mathbf{R}$ es tal que $g(x) = -x + 1$

Su representación es un subconjunto continuo de $\mathbf{R}^2$, consistente en una recta del plano.




Es fácil notar que, aunque se mantenga la ley de correspondencia o asignación, al variar el dominio o el codominio, la función cambia. En nuestro caso, $g \neq f$ aunque se cumple $f \subset g$. Es conveniente insistir entonces en el hecho de que la caracterización de una aplicación se da a través del dominio, codominio y la ley de asignación. En la terminología clásica, el elemento genérico $x$ del dominio se llama variable independiente, y su imagen $y = f(x)$ es lo que se conoce como variable dependiente.

*Ejemplo 4-6.*

Consideremos $A = \{ 1, 2 \}$, $B = \{ 1, 2, 3, 4 \}$ y la función

$$f : A^2 \to B$$

que asigna a cada elemento del dominio $A^2$, la suma de sus componentes, es decir

$$f(x, y) = x + y$$

a) Podemos confeccionar una tabla de simple entrada que especifique la imagen de cada punto del dominio

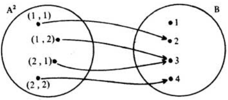
| $(x , y)$ | $f(x , y) = x + y$ |
|---|---|
| $(1 , 1)$ | 2 |
| $(1 , 2)$ | 3 |
| $(2 , 1)$ | 3 |
| $(2 , 2)$ | 4 |

El elemento 1 de B carece de antecedente o preimagen en A.

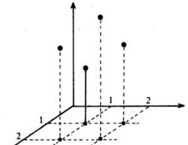
b) Otra representación de las imágenes se tiene mediante una tabla de doble entrada

| $f$ | 1 | 2 |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 4 |

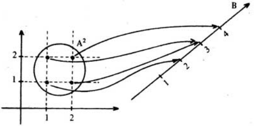
c) El diagrama de Venn es




d) La representación cartesiana es en el espacio, ya que cada elemento del dominio determina un punto del plano, y su imagen debe tomarse sobre otro eje.



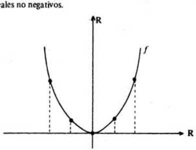
**e)** La misma función puede representarse de la siguiente manera, desconectando el dominio del codominio




***Ejemplo 4-7.***

Sea $f: \mathbf{R} \to \mathbf{R}$ definida por $f(x) = x^2$

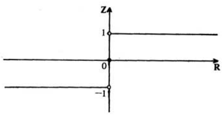
Como cada número real tiene un cuadrado y sólo uno, se cumplen las condiciones de la definición. El gráfico cartesiano es una línea continua de puntos del plano, llamada parábola. Hemos señalado algunos pares ordenados de $f$, los que se han unido mediante un trazo continuo. Como el cuadrado de ningún número real es negativo, las imágenes son reales no negativos.




***Ejemplo 4-8.***

Representación de $f: \mathbf{R} \to \mathbf{Z}$ definida de la siguiente manera

$$f(x) = \begin{cases} -1 & \text{si } x < 0 \\ 0 & \text{si } x = 0 \\ 1 & \text{si } x > 0 \end{cases}$$




Es la llamada función "signo de $x$", y su representación consiste en la unión de dos semirrectas abiertas (sin origen), con el conjunto cuyo único elemento es el origen de coordenadas.

## 4.4. CLASIFICACION DE FUNCIONES

Sea una función $f : A \to B$

Si ocurre que elementos distintos del dominio tienen imágenes distintas en el codominio, entonces $f$ se llama función inyectiva, biunívoca, o uno a uno.

Por otra parte, si todo elemento del codominio es imagen de algún elemento del dominio, la función se llama sobreyectiva.

Cuando se presentan ambas situaciones simultáneamente, la función se llama biyectiva o correspondencia biunívoca.

i ) ***Definición***

$$f : A \to B \text{ es inyectiva} \Leftrightarrow \forall x' \, \forall x'' \in A : x' \neq x'' \Rightarrow f(x') \neq f(x'')$$

Equivalentemente, mediante la implicación contrarrecíproca, podemos decir

$$f : A \to B \text{ es inyectiva} \Leftrightarrow \forall x' \, \forall x'' \in A : f(x') = f(x'') \Rightarrow x' = x''$$

En la inyectividad no puede darse que elementos distintos del dominio den la misma imagen. Las funciones estudiadas en los ejemplos 4-1 i ) y 4-1 iii) no son inyectivas. Tampoco lo son las correspondientes a 4-2 y 4-3. En cambio son inyectivas las funciones de los ejemplos 4-4 y 4-5.

En el diagrama de Venn correspondiente a una aplicación inyectiva no puede presentarse ninguna bifurcación de elementos del dominio hacia el codominio. En la representación plana cartesiana no puede ocurrir que una ordenada corresponda a más de una abscisa.

ii ) ***Definición***

$$f : A \to B \text{ es sobreyectiva} \Leftrightarrow \forall y \in B \,,\, \exists x \in A \,/\, y = f(x)$$

En el caso de sobreyectividad, el conjunto de las imágenes se identifica con el codominio de la función.

Los ejemplos 4-2 y 4-3 corresponden a funciones no sobreyectivas. En cambio lo son en 4-4 y 4-5.

Es usual nombrar a las funciones sobreyectivas con las palabras "sobre" o "suryectiva".

iii) ***Definición***

$f: A \to B$ es biyectiva $\Leftrightarrow f$ es inyectiva y $f$ es sobreyectiva.

Las funciones propuestas en los ejemplos 4-4 y 4-5 son biyectivas.

Negando el antecedente y consecuente de la doble implicación se tiene

$f: A \to B$ no es biyectiva $\Leftrightarrow f$ no es inyectiva o $f$ no es sobreyectiva.

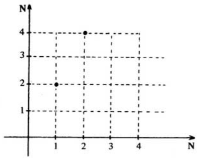
***Ejemplo 4-9.***

Representamos y clasificamos la función

$$f: \mathbf{N} \to \mathbf{N} \text{ tal que } f(x) = 2x$$

Esta función asigna a cada número natural su duplo. El conjunto de las imágenes es el de los números naturales pares, y está incluido en **N**, como codominio.

Su representación es un conjunto de puntos aislados del primer cuadrante.




Vamos a probar la inyectividad de $f$. Sean $x'$ y $x''$ en **N** tales que $f(x') = f(x'')$.

Esto significa que $2x' = 2x''$ y, en consecuencia, $x' = x''$. De modo que $f$ es inyectiva o 1–1 (uno a uno).

Además $f$ no es sobreyectiva, pues los elementos del codominio que son impares carecen de antecedente en **N**. Resulta que $f$ no es biyectiva.

*Ejemplo 4-10.*

Consideremos ahora el conjunto P de los números naturales pares, y

$$f: \mathbf{N} \to \mathbf{P} \ \text{tal que} \ f(x) = 2x$$

La ley de asignación es la misma que en 4-8, pero el codominio se ha "restringido" a los naturales pares. La inyectividad se mantiene y probamos la sobreyectividad.

Hay que determinar si para todo $y \in P$ existe $x$ en N tal que $f(x) = y$. Esto significa que debe ser, de acuerdo con la definición de $f$,

$$2x = y$$

Resulta $x = \frac{y}{2} \in \mathbf{N}$, pues la mitad de un número natural par es un número natural.

De modo que $\forall y \in P, \exists x = \frac{y}{2}$ tal que $f(x) = f\left(\frac{y}{2}\right) = 2 \cdot \frac{y}{2} = y$.

Siendo $f$ inyectiva y sobreyectiva resulta biyectiva.

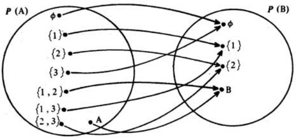
*Ejemplo 4-11.*

Sean $A = \left\{1, 2, 3\right\}$ y $B = \left\{1, 2\right\}$

Definimos $f: P(A) \to P(B)$ mediante $f(X) = X \cap B$

Es decir, la imagen de todo subconjunto de A es su intersección con B.

El siguiente diagrama nos muestra que $f$ es sobreyectiva, pero no inyectiva.



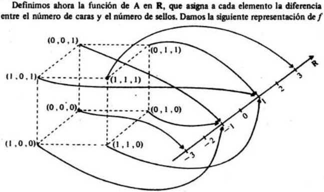

*Ejemplo 4-12.*

Se lanza una moneda tres veces. Los posibles resultados de este experimento aleatorio son todas las ternas formadas por "caras" y "sellos", o bien por "unos" y "ceros", y son los siguientes:

$$A = \{(1,1,1), (1,1,0), (1,0,1), (0,1,1), (1,0,0), (0,1,0), (0,0,1), (0,0,0)\}$$

El conjunto A de tales elementos, se llama espacio muestral asociado al experimento.

Definimos ahora la función de A en **R**, que asigna a cada elemento la diferencia entre el número de caras y el número de sellos. Damos la siguiente representación de $f$




$f$ no es inyectiva ni sobreyectiva.

***Ejemplo 4-13.***

Sea $f: \mathbf{R} \to \mathbf{R}$ definida por $f(x) = x^3$.

i ) $f$ es 1−1. En efecto, sean $x_1$ y $x_2$ en **R** tales que $f(x_1) = f(x_2)$ es decir $x_1^3 = x_2^3$. Por pasaje de términos

$$x_1^3 - x_2^3 = 0$$

factorizando la diferencia de cubos

$$(x_1 - x_2)(x_1^2 + x_1 x_2 + x_2^2) = 0$$

$$\Downarrow$$

$$x_1 - x_2 = 0 \Rightarrow x_1 = x_2$$

O bien

$$x_1^2 + x_1 x_2 + x_2^2 = 0$$

La relación que vincula a $x_1$ con $x_2$ está dada por

$$x_1 = \frac{-x_2 \pm \sqrt{x_2^2 - 4x_2^2}}{2} = \frac{-x_2 \pm \sqrt{-3x_2^2}}{2}$$

Es decir

$$x_1 = \left(\frac{-1}{2} \pm i\frac{\sqrt{3}}{2}\right) x_2 \qquad (1)$$

Si $x_2 = 0$ entonces $x_1 = 0$ y resulta $x_1 = x_2$

Estos son los únicos valores reales que satisfacen (1) y, en consecuencia, $f$ es inyectiva.

ii ) $f$ es sobreyectiva, pues

$$\forall y \in \mathrm{R}\ ,\ \exists\, x = \sqrt[3]{y} \text{ tal que}$$

$$f(x) = f(\sqrt[3]{y}) = (\sqrt[3]{y})^3 = y$$

Ocurre entonces que $f$ es biyectiva.

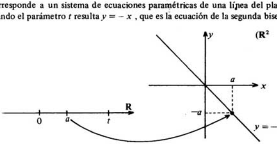
*Ejemplo 4-14.*

Sea $f : \mathbf{R} \to \mathbf{R}^2$ tal que $f(t) = (t, -t)$.

Si en $\mathbf{R}^2$ consideramos ejes $x$ e $y$, de acuerdo con la definición, se tiene

$$\begin{cases} x = t \\ y = -t \end{cases}$$

que corresponde a un sistema de ecuaciones paramétricas de una línea del plano $xy$. Eliminando el parámetro $t$ resulta $y = -x$ , que es la ecuación de la segunda bisectriz.




Es claramente una función inyectiva, pero no sobreyectiva.

## 4.5. FUNCIONES ESPECIALES

### 4.5.1. Función constante

La función $f$ : A → B, que asigna a todos los elementos del dominio el elemento $b \in$ B, se llama constante.

Está definida por $f(x) = b$ para todo $x \in$ A

Se tiene

$$f=\left\{(x\ ,b)\ /\ x \in A\right\}$$

A menos que A sea unitario, la función constante no es inyectiva, y es sobreyectiva sólo si B se reduce a un único elemento.

### 4.5.2. **Función identidad**

Identidad en A es la aplicación

$$i_A : A \rightarrow A \text{ tal que } i_A\,(x) = x$$

La identidad en A es entonces la función que asigna a cada elemento de A el mismo elemento, es decir, deja invariantes a los objetos de A.

A cada conjunto le corresponde una función identidad, y a veces en lugar de denotarla mediante $i_A$ se utiliza el símbolo $1_A$.

Se tiene

$$i_A = \left\{(x\ ,x)\ /\ x \in A\right\}$$

Es decir, la identidad en A es la diagonal de $A^2$. Es fácil verificar que, como relación, es reflexiva, simétrica y transitiva, o sea, de equivalencia en A; además es antisimétrica, y en consecuencia de orden amplio. La función $i_A$ es obviamente biyectiva.

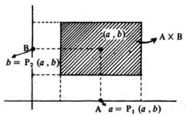
### 4.5.3. **Función proyección**

Consideremos A X B, y las funciones

$$P_1 : A \times B \rightarrow A$$
$$P_2 : A \times B \rightarrow B \qquad \text{definidas por}$$
$$P_1\,(a\ ,b) = a \qquad \text{y} \qquad P_2\,(a\ ,b) = b$$

Tales funciones se llaman primera y segunda proyección del producto cartesiano, y asignan a cada par ordenado la primera y segunda componente, respectivamente.

En un gráfico cartesiano se tiene



### 4.5.4. Función canónica

Sea $\sim$ una relación de equivalencia definida en el conjunto no vacío A. Por el teorema fundamental de las relaciones de equivalencia queda determinado el conjunto cociente $\frac{A}{\sim}$, cuyos elementos son las clases de equivalencia.

*Definición*

Aplicación canónica es la función

$$\varphi : A \to \frac{A}{\sim}$$

que asigna a cada elemento de A, su clase de equivalencia, es decir, tal que

$$\varphi(x) = K_x$$

Dos elementos equivalentes pertenecen a la misma clase y en consecuencia admiten la misma imagen, es decir, la aplicación canónica no es inyectiva, salvo en el caso de clases unitarias. Por otra parte, como cada clase es no vacía, ocurre que siempre es sobreyectiva, es decir

$$\forall K_u \in \frac{A}{\sim}, \exists x \in A / \varphi(x) = K_u$$

Vale la siguiente proposición

$$a \sim b \Leftrightarrow \varphi(a) = \varphi(b)$$

La función canónica en el caso de la congruencia módulo 3 definida en $\mathbf{Z}$ es $\varphi : \mathbf{Z} \to \mathbf{Z}_3$ tal que $\varphi(x) = K_u$, siendo $u$ el resto de la división de $x$ por 3.

*Ejemplo 4-15.*

En $\mathbf{R}^2$ consideramos la relación definida por

$$(a, b) \sim (a', b') \Leftrightarrow a = a'$$

Es decir, dos pares ordenados de reales están relacionados si y sólo si tienen la misma primera componente. Puede verificarse fácilmente que la relación es de equivalencia, y el propósito consiste en caracterizar la aplicación canónica. Las clases de equivalencia son del tipo

$$K_{(a,b)} = \left\{ (x, y) / x = a \right\}$$

y están representadas por paralelas al eje de ordenadas. Para definir el conjunto cociente necesitamos un conjunto de índices, y al elegir un único elemento en cada clase, lo tomamos sobre el eje de abscisas, de modo que

$$\frac{\mathbf{R}^2}{\sim} = \left\{ K_{(u,0)} / u \in \mathbf{R} \right\}$$

Entonces la función canónica es $\varphi : \mathbf{R}^2 \rightarrow \dfrac{\mathbf{R}^2}{\sim}$ tal que

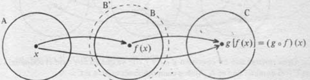
$$\varphi(a\,,\,b) = K_{(u\,,\,o)} \quad \text{si} \quad u = a$$

## 4.6. COMPOSICION DE FUNCIONES

Bajo ciertas condiciones es posible definir, a partir de dos funciones $f$ y $g$, una nueva función, llamada la compuesta de aquéllas.

Sean

$$f : A \rightarrow B \quad \text{y} \quad g : B \rightarrow C$$




donde coinciden el codominio de la primera con el dominio de la segunda. Si bien consideramos este caso más usual, es suficiente que el codominio de la primera sea parte del dominio de la segunda, es decir: $B \subset B'$.

Nuestro propósito es asignar a cada elemento de A un único elemento de C, y el camino natural consiste en determinar la imagen de cualquier $x \in A$ por $f$, y a continuación obtener la imagen de $f(x) \in B$, por $g$.

*Definición*

Composición de las funciones $f : A \rightarrow B$ y $g : B \rightarrow C$ es la función $g \circ f : A \rightarrow C$, definida por

$$(g \circ f)(x) = g\,[f(x)] \quad \text{para todo} \quad x \in A$$

El símbolo "$g \circ f$" denota la función compuesta de $f$ con $g$, o la composición de $f$ con $g$. Puede leerse "$f$ compuesta con $g$", o "$g$ cerito $f$" o bien "$g \circ f$".

*Ejemplo 4-16.*

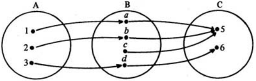
Sean $A = \{1\,,2\,,3\}$, $B = \{a\,,b\,,c\,,d\}$, $C = \{5\,,6\}$ y las funciones $f : A \rightarrow B$ y $g : B \rightarrow C$ definidas así

$$f = \{(1, a), (2, b), (3, d)\}$$
$$g = \{(a, 5), (b, 5), (c, 5), (d, 6)\}$$

Resulta

$$g \circ f = \{(1, 5), (2, 5), (3, 6)\}$$

El diagrama correspondiente es




Debe notarse que no coexisten $g \circ f$ y $f \circ g$, ya que en este caso el codominio de $g$ es C y el dominio de $f$ es A. Ambas composiciones existen si $C \subset A$.

***Ejemplo 4-17.***

Sean ahora las funciones

$$f : \mathbf{R} \rightarrow \mathbf{R} \text{ tal que } f(x) = 2x$$
$$g : \mathbf{R} \rightarrow \mathbf{R} \text{ tal que } g(x) = x^2$$

Entonces

i ) $g \circ f : \mathbf{R} \rightarrow \mathbf{R}$ está definida por

$$(g \circ f)(x) = g[f(x)] = g(2x) = (2x)^2 = 4x^2$$

ii ) $f \circ g : \mathbf{R} \rightarrow \mathbf{R}$ está definida por

$$(f \circ g)(x) = f[g(x)] = f(x^2) = 2x^2$$

Ambas funciones compuestas, a pesar de tener el mismo dominio y codominio, son distintas, por diferir en la ley de asignación.

***Definición***

Dos funciones $f : A \rightarrow B$ y $g : A \rightarrow B$ son iguales si y sólo si para todo $x$ de A se verifica $f(x) = g(x)$.

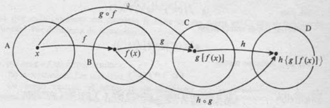
Con relación al ejemplo se tiene: $g \circ f \neq f \circ g$.

**4.6.2. Asociatividad de la composición**

Sean $f : A \to B$, $g : B \to C$ y $h : C \to D$.
Entonces se verifica

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Las dos composiciones son funciones de A en D, y se trata de probar la igualdad. Interpretamos la situación en el siguiente diagrama




Con relación al primer miembro se tiene

$$\left.\begin{array}{r} f : A \to B \\ h \circ g : B \to D \end{array}\right\} \Rightarrow (h \circ g) \circ f : A \to D$$

Para el segundo miembro es

$$\left.\begin{array}{r} g \circ f : A \to C \\ h : C \to D \end{array}\right\} \Rightarrow h \circ (g \circ f) : A \to D$$

Siendo $(h \circ g) \circ f$ y $h \circ (g \circ f)$ dos aplicaciones con el mismo dominio y codominio, para probar la igualdad, de acuerdo con la definición expuesta en 4.6.1., hay que verificar la igualdad de imágenes para todo elemento de A, dadas por dichas funciones.

Sea $x \in A$; aplicando reiteradamente la definición de composición

$$\Big((h \circ g) \circ f\Big)(x) = (h \circ g)\Big(f(x)\Big) = h\left\{g\,[f(x)]\right\} \qquad (1)$$

Por otra parte

$$\Big(h \circ (g \circ f)\Big)(x) = h\Big((g \circ f)(x)\Big) = h\left\{g\,[f(x)]\right\} \qquad (2)$$

De (1) y (2) se deduce

$$\Big((h \circ g) \circ f\Big)(x) = \Big(h \circ (g \circ f)\Big)(x) \quad \forall x \in A$$

Y por definición de igualdad de funciones resulta

$$(h \circ g) \circ f = h \circ (g \circ f)$$

### 4.6.3. Composición de funciones inyectivas

Si $f : A \to B$ y $g : B \to C$ son inyectivas, entonces $g \circ f : A \to C$ es inyectiva.

De acuerdo con la definición de inyectividad 4.4. i ) debemos probar que si $x'$ y $x''$ son elementos de A que tienen la misma imagen por $g \circ f$, entonces $x' = x''$.

Sea pues $$(g \circ f)(x') = (g \circ f)(x'').$$

Por definición de composición

$$g[f(x')] = g[f(x'')]$$

Por ser $g$ inyectiva resulta

$$f(x') = f(x'')$$

ya que estos elementos de B tienen la misma imagen por $g$. Y por ser $f$ inyectiva:

$$x' = x''$$

Queda probado, así, que la composición de funciones inyectivas es inyectiva.

### 4.6.4. Composición de funciones sobreyectivas

Si $f : A \to B$ y $g : B \to C$ son sobreyectivas, entonces $g \circ f : A \to C$ es sobreyectiva.

Según 4.4. ii ) hay que probar que para todo $z \in C$ existe $x \in A$ tal que $(g \circ f)(x) = z$.

Por ser $g: B \to C$ sobreyectiva,

$$\forall z \in C, \exists y \in B / g(y) = z$$

Ahora bien, dado $y \in B$, por ser $f : A \to B$ sobreyectiva,

$$\exists x \in A / f(x) = y$$

De aquí se deduce que

$$g[f(x)] = g(y) = z$$

Entonces, dado cualquier $z \in C$, $\exists\, x \in A$ tal que $(g \circ f)(x) = z$, de acuerdo con la definición de composición.

En consecuencia, la composición de funciones sobreyectivas es sobreyectiva.

### 4.6.5. Composición de funciones biyectivas

Si $f : A \to B$ y $g : B \to C$ son biyectivas, entonces la composición $g \circ f : A \to C$ es biyectiva.

Este enunciado es una consecuencia de 4.6.3. y 4.6.4.

***Ejemplo 4-18.***

En 4.6.3. se ha demostrado que la composición de dos aplicaciones inyectivas es inyectiva. La inyectividad de la composición no implica la de cada función, pero sí la de la primera. Es decir, si $f: A \to B$ y $g: B \to C$ son tales que $g \circ f: A \to C$ es 1–1, entonces $f$ es inyectiva.

Sean $x'$ y $x''$ en A tales que $f(x') = f(x'')$. Hallando la imagen de éste elemento de B por $g$, se tiene

$$g[f(x')] = g[f(x'')]$$

ya que cada elemento del dominio B tiene imagen única en C, por definición de función. Por definición de composición

$$(g \circ f)(x') = (g \circ f)(x'')$$

y, por ser $g \circ f$ inyectiva, resulta $x' = x''$.

En consecuencia, $f$ es inyectiva.

De modo análogo el lector puede demostrar que si la composición de dos aplicaciones es sobreyectiva, entonces la segunda es sobreyectiva.

## 4.7. FUNCIONES INVERSAS

Toda función $f: A \to B$ es una relación; cabe preguntarse si la relación inversa es una función. En general, la respuesta es negativa, como se ve a través del ejemplo 4-2, donde $A = \{-1, 0, 1, 2\}$, $B = \{0, 1, 2, 3, 4\}$ y $f: A \to B$ es tal que $f(x) = x^2$, es decir

$$f = \{(-1, 1), (0, 0), (1, 1), (2, 4)\}$$

La inversa de esta relación es el subconjunto de $B \times A$:

$$\{(1, -1), (0, 0), (1, 1), (4, 2)\}$$

Se ve claramente que esta relación no es una función de B en A, pués los elementos 2 y 3 del eventual dominio carecen de imágenes en A, y además no se cumple la condición de unicidad, ya que 1 tiene dos correspondientes en A.

Sea en cambio el siguiente caso $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ y $f = \{(1, a), (2, c), (3, b)\}$ una función de A en B. La relación inversa es

$$g = \{(a, 1), (b, 3), (c, 2)\}$$

es claramente una función de B en A, llamada función inversa de $f$. La composición

$$g \circ f = \{(1, 1), (2, 2), (3, 3)\} = i_A$$

y

$$f \circ g = \{(a, a), (b, b), (c, c)\} = i_B$$

***Definición***

La función $f: A \to B$ admite inversa si y sólo si existe $g: B \to A$ tal que $g \circ f = i_A$ y $f \circ g = i_B$

***Ejemplo 4-19.***

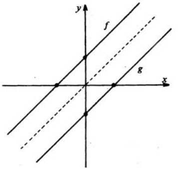
La función $f: \mathbf{R} \to \mathbf{R}$ definida por $f(x) = x + 2$ admite inversa $g: \mathbf{R} \to \mathbf{R}$ tal que $g(x) = x - 2$, pues

$$(g \circ f)(x) = g[f(x)] = g(x + 2) = x + 2 - 2 = x = i_{\mathbf{R}}(x)$$
$$(f \circ g)(x) = f[g(x)] = f(x - 2) = x - 2 + 2 = x = i_{\mathbf{R}}(x)$$

según las definiciones de composición, de $f$, de $g$ y de identidad. Por igualdad de funciones resulta

$$g \circ f = i_{\mathbf{R}} \ \text{ y } \ f \circ g = i_{\mathbf{R}}$$

La representación cartesiana de dos funciones inversas conduce a gráficos simétricos respecto de la primera bisectriz:




La función $f$ es biyectiva, como puede probarse fácilmente, y este hecho es necesario y suficiente para que admita inversa.

**4.7.2. Propiedad**

Una función admite inversa si y sólo si es biyectiva.

I) Si una función admite inversa, entonces es biyectiva.

Hipótesis) $f: A \to B$ es tal que existe $g: B \to A$ siendo $g \circ f = i_A$ y $f \circ g = i_B$

Tesis) $f$ es biyectiva.

Demostración)

a) Vemos primero la inyectividad de $f$.

Sean $x'$ y $x''$ en A tales que $f(x') = f(x'')$. La imagen de este elemento de B por $g$ es

$$g[f(x')] = g[f(x'')]$$

Por definición de composición, esto se traduce en

$$(g \circ f)(x') = (g \circ f)(x'')$$

y siendo por hipótesis $g \circ f = i_A$, se tiene

$$i_A(x') = i_A(x'')$$

Es decir: $x' = x''$, lo que demuestra que $f$ es $1 - 1$.

b) Demostramos ahora que $f$ es sobreyectiva.

De acuerdo con la definición, debemos probar la verdad de la proposición siguiente

$$\forall y \in B \ , \ \exists \ x \in A \ / \ f(x) = y$$

Sea entonces cualquier elemento $y \in B$; por definición de identidad en B se tiene

$$y = i_B(y) \quad , \quad \text{y como por hipótesis} \quad i_B = f \circ g$$

se tiene

$$y = (f \circ g)(y)$$

Por definición de composición

$$y = f[g(y)]$$

Es decir, a expensas de $y \in B$, hemos determinado $x = g(y)$ en A, tal que $f(x) = y$.

Siendo $f$ inyectiva y sobreyectiva resulta biyectiva.

II) Si una función es biyectiva, entonces admite inversa.

Hipótesis) $f: A \to B$ es biyectiva.

Tesis) $\exists \ g: B \to A$ tal que $g \circ f = i_A$ y $f \circ g = i_B$.

Demostración) Necesitamos proceder en tres etapas.

a) Primero se trata de definir una función $g: B \to A$, de modo que se verifiquen las restantes proposiciones de la tesis.

En este sentido, definimos

$$g: B \to A \quad \text{mediante} \quad g(y) = x \quad \text{si} \quad f(x) = y \qquad (1)$$

Tenemos que ver que (1) satisface la definición de función. En efecto:

i) Todo elemento $y$ del dominio B tiene un correspondiente $x$ en A, ya que, por ser $f$ sobreyectiva, todo $y \in B$ proviene de algún $x \in A$.

ii ) El correspondiente $x$ asociado a $y$ es único, por ser $f$ inyectiva.

En efecto, si $x$ y $x'$ fueran antecedentes distintos de $y$ por $f$ se tendría $x \neq x' \ \wedge \ f(x) = f(x') = y$, lo que es absurdo por la inyectividad de $f$.

b) Hay que probar que $g \circ f = i_A$.

Cualquiera que sea $x$ en A se tiene, por definición de composición, por (1), y por definición de identidad en A

$$(g \circ f)(x) = g[f(x)] = g(y) = x = i_A(x)$$

Entonces, por definición de funciones iguales

$$g \circ f = i_A$$

c) Finalmente, demostramos que $f \circ g = i_B$.

Como $f \circ g : B \to B$, para todo $y \in B$, tenemos, por definición de composición, por (1) y por identidad en B

$$(f \circ g)(y) = f[g(y)] = f(x) = y = i_B(y)$$

Es decir

$$f \circ g = i_B$$

### 4.7.3. Consecuencia

Si $f : A \to B$ es biyectiva, entonces la función $g : B \to A$ a que se refiere el teorema anterior es única y, además, biyectiva.

Si existieran dos funciones $g$ y $g'$ que cumplieran las condiciones de 4.7.2. II) se tendría

$$g' = g' \circ i_B = g' \circ (f \circ g) = (g' \circ f) \circ g = i_A \circ g = g$$

por ser $i_B$ neutro a derecha e igual a $f \circ g$, por asociatividad de la composición, por ser $g' \circ f = i_A$, y porque $i_A$ es neutro a izquierda. En consecuencia, $g$ es única.

Por otra parte, de acuerdo con 4.7.2. I) se tiene esta situación: $g : B \to A$ es tal que existe $f : A \to B$, siendo $f \circ g = i_B$ y $g \circ f = i_A$. En consecuencia, $g$ es biyectiva.

La función $g$ se llama la inversa de $f$ y se denota con el símbolo $f^{-1}$

*Ejemplo 4-20.*

Se trata de probar que

$$f : \mathbf{R} \to (-1, 1) \text{ definida por}$$

$$f(x) = \frac{x}{1 + |x|} \quad \text{admite inversa.}$$

De acuerdo con el teorema anterior es suficiente probar que $f$ es biyectiva.

Previamente, necesitamos precisar algunos conceptos relativos a la función valor absoluto, y su conexión con la función signo.

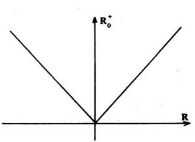
i ) Función valor absoluto es la aplicación

$$|\ |: \mathbf{R} \to \mathbf{R}_0^+ \quad (\text{ siendo } \mathbf{R}_0^+ = \mathbf{R}^+ \cup \{0\})$$

definida por

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$$

Su representación cartesiana consiste en el par de bisectrices del primero y segundo cuadrante. La función valor absoluto es sobreyectiva, pero no inyectiva.




ii ) Función "signo de $x$" es la aplicación

$$sg: \mathbf{R} \to \mathbf{Z} \quad \text{definida por}$$

$$sg(x) = \begin{cases} 1 & \text{si } x > 0 \\ 0 & \text{si } x = 0 \\ -1 & \text{si } x < 0 \end{cases}$$

Esta función ya fue graficada en el ejemplo 4-8.

iii) Cualquiera que sea el número real $x$, se cumple

$$|x| = x \,.\, sg(x)$$

lo que es fácil de verificar teniendo en cuenta las definiciones de valor absoluto y de signo de $x$.

Retomamos nuestro propósito inicial:

a) $f$ es inyectiva.

Sean $x'$ y $x''$ en A, tales que

$$f(x') = f(x'')$$
$$\Downarrow$$
$$\frac{x'}{1+|x'|} = \frac{x''}{1+|x''|} \quad \text{con} \quad sg\,(x') = sg\,(x'')$$
$$\Downarrow$$
$$x' + x'\,|x''| = x'' + x''\,|x'| \quad \text{y} \quad sg\,(x') = sg\,(x'')$$
$$\Downarrow$$
$$x' + x' .\, x''\, sg\,(x'') = x'' + x'' .\, x'\, sg\,(x') \quad \text{Por iii)}$$
$$\Downarrow$$
$$x' = x''$$

O sea: $f$ es $1-1$.

b) $f$ es sobreyectiva.

Sea $y \in (-1\,,1)$. Si $\exists\, x \in \mathbf{R} \,/\, f(x) = y$, entonces debe ser

$$\frac{x}{1+|x|} = y \quad \text{con} \quad sg\,(x) = sg\,(y) \qquad (1)$$

Operando

$$x = y + y\,|x| \qquad \text{Por (1)}$$
$$\Downarrow$$
$$x = y + y\,x\,sg\,(x) \qquad \text{Por iii)}$$
$$\Downarrow$$
$$x = y + x\,y\,sg\,(y) \qquad \text{Por (1)}$$
$$\Downarrow$$
$$x - x\,y\,sg\,(y) = y \qquad \text{Por trasposición}$$
$$\Downarrow$$
$$x\,(1 - |y|) = y \qquad \text{Por distributividad y iii)}$$
$$\Downarrow$$
$$x = \frac{y}{1-|y|} \qquad \text{Pues } 1 - |y| > 0 \text{ ya que } |y| < 1$$

Es decir

$$\forall\, y \in (-1\,,1)\,,\ \exists\ x = \frac{y}{1-|y|}$$

tal que

$$f(x) = f\left(\frac{y}{1-|y|}\right) = \frac{\dfrac{y}{1-|y|}}{1+\left|\dfrac{y}{1-|y|}\right|} =$$

$$= \frac{\dfrac{y}{1-|y|}}{1+\dfrac{|y|}{1-|y|}} = \frac{y}{1-|y|+|y|} = y$$

Esto prueba que $f$ es sobreyectiva.

Por a) y b) resulta que $f$ es biyectiva y en consecuencia admite inversa. La inversa es

$$f^{-1} : (-1\,,\,1) \to \mathbf{R} \text{ tal que}$$
$$f^{-1}(x) = \frac{x}{1-|x|}$$

c) Verificamos que $g \circ f = i_{\mathbf{R}}$

En efecto

$$\forall x \in \mathbf{R} : (g \circ f)(x) = g\,[f(x)] =$$

$$= g\left(\frac{x}{1+|x|}\right) = \frac{\dfrac{x}{1+|x|}}{1-\left|\dfrac{x}{1+|x|}\right|} = x = i_{\mathbf{R}}(x)$$

d) Además, $f \circ g = i_{(-1,1)}$

Pues

$$x \in i_{(-1,1)} \Rightarrow (f \circ g)(x) = f\,[g(x)] =$$

$$= f\left(\frac{x}{1-|x|}\right) = \frac{\dfrac{x}{1-|x|}}{1+\left|\dfrac{x}{1-|x|}\right|} = x =$$

$$= i_{(-1,1)}(x)$$

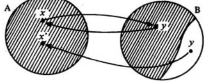
***Ejemplo 4-21.***

La función $f : A \to B$ es inyectiva si y sólo si existe $g : B \to A$ tal que $g \circ f = i_A$

I) Hipótesis) $f : A \to B$ es 1–1.

Tesis) $\exists\, g : B \to A$ tal que $g \circ f = i_A$.

Demostración) La función $f$ no es necesariamente sobreyectiva, de modo que eventualmente existen elementos del codominio sin preimagen en el dominio. Nos ayudamos con el siguiente diagrama




Definimos una función $g: B \rightarrow A$ mediante la siguiente asignación

$$g(y) = \begin{cases} x & \text{si } f(x) = y \\ x' & \text{(Cualquier elemento fijo de A) si no existe } x \in A \text{ tal que } f(x) = y. \end{cases}$$

De este modo, todo elemento d B tiene un correspondiente en A, y además es único, por ser $f$ inyectiva.

Ahora bien, utilizando las definiciones de composición, de $g$, y de identidad en A, se tiene, cualquiera que sea $x \in A$

$$(g \circ f)(x) = g[f(x)] = g(y) = x = i_A(x)$$

y por definición de funciones iguales resulta

$$g \circ f = i_A$$

II) Hipótesis) $f: A \rightarrow B$ es tal que existe $g: B \rightarrow A$ de modo que $g \circ f = i_A$

Tesis) $f$ es inyectiva.

Demostración) Sean $x'$ y $x''$ en A tales que $f(x') = f(x'')$.

Entonces: $g[f(x')] = g[f(x'')]$

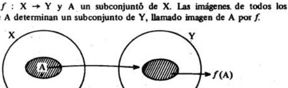
Por definición de composición: $(g \circ f)(x') = (g \circ f)(x'')$.

Por hipótesis: $i_A(x') = i_A(x'')$.

Esto implica $x' = x''$, y en consecuencia $f$ es $1-1$.

## 4.8. IMAGENES DE SUBCONJUNTOS DEL DOMINIO

4.8.1. Sean $f: X \rightarrow Y$ y A un subconjuntö de X. Las imágenes de todos los elementos de A determinan un subconjunto de Y, llamado imagen de A por $f$.



***Definición***

**Imagen del subconjunto $A \subset X$ es el conjunto cuyos elementos son las imágenes de los elementos de A.**

En símbolos

$$f(A) = \left\{ f(x) \,/\, x \in A \right\}$$

O bien

$$f(A) = \left\{ y \in Y \,/\, \exists\, x \in A \ \wedge \ f(x) = y \right\}$$

El símbolo $f(A)$ se lee "imagen de A".

De acuerdo con la definición

$$y \in f(A) \Leftrightarrow \exists\, x \in A \,/\, y = f(x)$$

En particular, si $A = X$, entonces $f(X)$ se llama imagen del dominio por $f$ o directamente imagen de $f$. Además, $f(\phi) = \phi$.

Se tiene obviamente que $f$ es sobreyectiva si y sólo si $f(X) = Y$.

### 4.8.2. Propiedades de la imagen

Sean $f: X \to Y$ y A y B subconjuntos del dominio.

a) Si un subconjunto del dominio es parte de otro, entonces la misma relación vale para sus imágenes.

Es decir, si $f: X \to Y$, $A \subset X$, $B \subset X$ y $A \subset B$, entonces es $f(A) \subset f(B)$.

En efecto, sea

| | |
|---|---|
| $z \in f(A)$ | |
| $\Downarrow$ | |
| $\exists\, x \in A \,/\, f(x) = z$ | Por definición de imagen |
| $\Downarrow$ | |
| $\exists\, x \in B \,/\, f(x) = z$ | Por ser $A \subset B$ |
| $\Downarrow$ | |
| $z \in f(B)$ | Por definición de imagen |

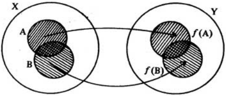
b) La imagen de la unión de dos subconjuntos del dominio, es igual a la unión de sus imágenes.

Hipótesis) $f: X \to Y$

$A \subset X$ y $B \subset X$

Tesis) $f(A \cup B) = f(A) \cup f(B)$

Demostración)




Probamos la doble inclusión.

1°) Sea

$$z \in f(A \cup B)$$
$$\Downarrow$$
$$\exists\, x \in A \cup B \,/\, f(x) = z$$
$$\Downarrow$$
$$\exists\, x \,/\, (x \in A \ \vee \ x \in B) \ \wedge \ f(x) = z$$
$$\Downarrow$$
$$(\exists x \ / \ x \in A \ \wedge f(x) = z) \ \vee \ (\exists x / x \in B \ \wedge \ f(x) = z)$$
$$\Downarrow$$
$$z \in f(A) \ \vee \ z \in f(B)$$
$$\Downarrow$$
$$z \in f(A) \cup f(B)$$

Es decir

$$f(A \cup B) \subset f(A) \cup f(B) \qquad (1)$$

2°) Usando propiedades de la inclusión y a)

$$\left.\begin{array}{l} A \subset A \cup B \Rightarrow f(A) \subset f(A \cup B) \\ B \subset A \cup B \Rightarrow f(B) \subset f(A \cup B) \end{array}\right\} \Rightarrow$$
$$\Rightarrow f(A) \cup f(B) \subset f(A \cup B) \qquad (2)$$

De (1) y (2) resulta

$$f(A \cup B) = f(A) \cup f(B)$$

c) La imagen de la intersección de dos subconjuntos del dominio está incluida en la intersección de sus imágenes.

Se trata de ver que si $f : X \to Y$, $A \subset X$ y $B \subset X$, entonces

$$f(A \cap B) \subset f(A) \cap f(B)$$

En efecto, sea

$$z \in f(A \cap B)$$
$$\Downarrow$$
$$\exists x \in A \cap B / f(x) = z$$
$$\Downarrow$$
$$(\exists x \in A / f(x) = z) \ \wedge \ (\exists x \in B / f(x) = z)$$
$$\Downarrow$$
$$z \in f(A) \ \wedge \ z \in f(B)$$
$$\Downarrow$$
$$z \in f(A) \cap f(B)$$

Entonces

$$f(A \cap B) \subset f(A) \cap f(B)$$

El siguiente ejemplo prueba que no es válida la inclusión en el otro sentido.
Sean $f : \mathbf{Z} \to \mathbf{N}$ definida por

$$f(x) = x^2$$

y los subconjuntos de **Z**

$$A = \left\{-2, -3, 4\right\} \text{ y } B = \left\{2, 3, 4, 5\right\}$$

Se tiene $A \cap B = \left\{4\right\}$ y

$$f(A \cap B) = \left\{16\right\}$$
$$f(A) \cap f(B) = \left\{4, 9, 16\right\} \cap \left\{4, 9, 16, 25\right\} = \left\{4, 9, 16\right\}$$

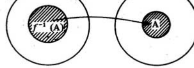
Resulta

$$f(A \cap B) \underset{\neq}{\subset} f(A) \cap f(B)$$

## 4.9. IMAGENES INVERSAS DE SUBCONJUNTOS DEL CODOMINIO

### 4.9.1. Concepto

Sean $f : X \to Y$ y A una parte del codominio Y. Un problema de interés consiste en determinar los elementos del dominio cuyas imágenes pertenecen a A. Tales elementos forman un subconjunto de X, llamado imagen inversa o preimagen de A por $f$




***Definición***

Imagen inversa o preimagen del subconjunto $A \subset Y$, es el conjunto de los elementos del dominio cuyas imágenes pertenecen a A.

La notación para indicar la preimagen de A por $f$, es $f^{-1}$ (A) y no debe entenderse que se indica la función inversa, la cual puede no existir, ya que nada se prefija acerca de $f$.

En símbolos

$$f^{-1}(A) = \{x \in X \,/\, f(x) \in A\}$$

Es claro que

$$x \in f^{-1}(A) \Leftrightarrow f(x) \in A$$

Es decir, un elemento del dominio pertenece a la preimagen de A si y sólo si su imagen pertenece a A.

***Ejemplo 4-22.***

Sea $f: \mathbf{R} \to \mathbf{R}$ definida por $f(x) = x^2$.

Determinamos las preimágenes de los siguientes subconjuntos del codominio

$$(-\infty, -1], (-1, 1], (-1, 1), [4, 9]$$

Se tiene

i ) $f^{-1}(-\infty, -1] = \{x \in \mathbf{R} \,/\, f(x) \in (-\infty, -1]\}$

Ahora bien

$$f(x) \in (-\infty, -1] \Leftrightarrow x^2 \leqslant -1 \Leftrightarrow x \in \phi$$

Resulta

$$f^{-1}(-\infty, -1] = \phi$$

ii ) En el segundo caso

| | |
|---|---|
| $x \in f^{-1}(-1\,,\,1]$ | |
| $\Updownarrow$ | |
| $f(x) \in (-1\,,1]$ | Por definición de preimagen |
| $\Updownarrow$ | |
| $x^2 \in (-1\,,1]$ | Por definición de $f$ |
| $\Updownarrow$ | |
| $-1 < x^2 \leq 1$ | Por definición de intervalo |
| $\Updownarrow$ | |
| $x^2 \leq 1$ | Pues $x^2 > -1\,,\ \forall\, x$ |
| $\Updownarrow$ | |
| $\lvert x\rvert^2 \leq 1$ | Porque $x^2 = \lvert x\rvert^2$ |
| $\Updownarrow$ | |
| $-1 \leq x \leq 1$ | Por ser $\lvert x\rvert \leq 1$ |
| $\Updownarrow$ | |
| $x \in [-1\,,1]$ | Por definición de intervalo cerrado |

Entonces $f^{-1}(-1\,,1] = [-1\,,1)$

iii) Se tiene

$$
\begin{gathered}
x \in f^{-1}(-1\,,1)\\
\Updownarrow\\
f(x) \in (-1\,,1)\\
\Updownarrow\\
x^2 \in (-1\,,1)\\
\Updownarrow\\
x^2 < 1\\
\Updownarrow\\
\lvert x\rvert < 1\\
\Updownarrow\\
-1 < x < 1\\
\Updownarrow\\
x \in (-1\,,1)
\end{gathered}
$$

Luego $f^{-1}(-1\,,1) = (-1\,,1)$

iv) Finalmente

$$x \in f^{-1}[4,9]$$
$$\Updownarrow$$
$$f(x) \in [4,9]$$
$$\Updownarrow$$
$$x^2 \in [4,9]$$
$$\Updownarrow$$
$$4 \leqslant x^2 \leqslant 9$$
$$\Updownarrow$$
$$x^2 \geqslant 4 \ \wedge \ x^2 \leqslant 9$$
$$\Updownarrow$$
$$|x| \geqslant 2 \ \wedge \ |x| \leqslant 3$$
$$\Updownarrow$$
$$x \in [-3,-2] \ \vee \ x \in [2,3]$$
$$\Updownarrow$$
$$x \in [-3,-2] \cup [2,3]$$

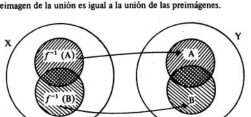
Entonces

$$f^{-1}[4,9] = [-3,-2] \cup [2,3]$$

### 4.9.2. Propiedades de la preimagen

Sean $f: X \to Y$ y los subconjuntos $A \subset Y, B \subset Y$

a) La preimagen de la unión es igual a la unión de las preimágenes.




Se trata de probar que $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$

Utilizamos sucesivamente las definiciones de preimagen, de unión y de preimagen:

$$x \in f^{-1}(A \cup B) \Leftrightarrow f(x) \in A \cup B \Leftrightarrow$$
$$\Leftrightarrow f(x) \in A \ \vee \ f(x) \in B \Leftrightarrow$$
$$\Leftrightarrow x \in f^{-1}(A) \ \vee \ x \in f^{-1}(B) \Leftrightarrow$$
$$\Leftrightarrow x \in f^{-1}(A) \cup f^{-1}(B)$$

b) La preimagen de la intersección es igual a la intersección de las preimágenes, es decir

$$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$$

Razonando análogamente, se tiene

$$x \in f^{-1}(A \cap B) \Leftrightarrow f(x) \in A \cap B \Leftrightarrow$$
$$\Leftrightarrow f(x) \in A \;\wedge\; f(x) \in B \Leftrightarrow$$
$$\Leftrightarrow x \in f^{-1}(A) \;\wedge\; x \in f^{-1}(B) \Leftrightarrow$$
$$\Leftrightarrow x \in f^{-1}(A) \cap f^{-1}(B)$$

c) La imagen inversa del complemento de un subconjunto del codominio es igual al complemento de su preimagen

$$f^{-1}(A^c) = [f^{-1}(A)]^c$$

En efecto

$$x \in f^{-1}(A^c) \Leftrightarrow f(x) \in A^c \Leftrightarrow f(x) \notin A \Leftrightarrow$$
$$\Leftrightarrow \sim [f(x) \in A] \Leftrightarrow \sim [x \in f^{-1}(A)] \Leftrightarrow$$
$$\Leftrightarrow x \notin f^{-1}(A) \Leftrightarrow x \in [f^{-1}(A)]^c$$

*Ejemplo 4-23.*

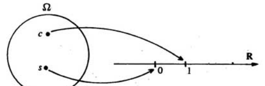
El conjunto $\Omega$ consiste en los posibles resultados que se obtienen al lanzar una moneda, es decir

$$\Omega = \{c, s\}$$

Se define $f : \Omega \to \mathbf{R}$ mediante

$$f(c) = 1$$
$$f(s) = 0$$

En un diagrama, la situación es



Determinar $f^{-1}(-\infty, x]$, $\forall x \in \mathbf{R}$
Por definición de preimagen

$$f^{-1}(-\infty, x] = \left\{ w \in \Omega / f(w) \leqslant x \right\}$$

Entonces

$$f^{-1}(-\infty, x] = \begin{cases} \phi & \text{si } x < 0 \\ \{s\} & \text{si } 0 \leqslant x < 1 \\ \{c, s\} & \text{si } 1 \leqslant x \end{cases}$$

***Ejemplo 4-24.***

Sea una aplicación

$$f: \mathrm{A} \to \mathbf{R}$$

Demostrar

$$\forall x \in \mathbf{R}: \bigcup_{n=1}^{\infty} f^{-1}(-\infty, x - 2^{-n}] = f^{-1}(-\infty, x)$$

Para cada $x \in \mathbf{R}$, el primer miembro denota la unión de una sucesión de conjuntos del dominio A, cuya identificación con la preimagen de $(-\infty, x)$ debemos probar.

i ) Sea $w \in \bigcup_{n=1}^{\infty} f^{-1}(-\infty, x - 2^{-n}]$

Por definición de unión, $\exists\ m \in \mathbf{N}$ tal que

$$w \in f^{-1}(-\infty, x - 2^{-m}]$$

Por definición de preimagen

$$f(w) \leqslant x - 2^{-m} \qquad (1)$$

Y como

$$0 < 2^{-m} \qquad (2)$$

Sumando (1) y (2)

$$f(w) < x$$

es decir: $f(w) \in (-\infty, x)$,
y por definición de preimagen resulta

$$w \in f^{-1}(-\infty, x)$$

Luego

$$\bigcup_{n=1}^{\infty} f^{-1}(-\infty, x - 2^{-n}] \subset f^{-1}(-\infty, x) \qquad (3)$$

ii ) Sea ahora

$$w \in f^{-1}(-\infty, x)$$

Por definición de preimagen

$$f(w) < x$$

Es decir: $x - f(w) > 0$

Y siendo $x - f(w)$ un número real positivo existe $m \in \mathbf{N}$ tal que

$$x - f(w) \geqslant 2^{-m}$$

Por trasposición de términos

$$f(w) \leqslant x - 2^{-m}$$

O sea

$$\exists\, m \in \mathbf{N} / f(w) \in (-\infty, x - 2^{-m}]$$

Y por definición de preimagen

$$\exists\, m \in \mathbf{N} / w \in f^{-1}(-\infty, x - 2^{-m}]$$

Por definición de unión resulta

$$w \in \bigcup_{n=1}^{\infty} f^{-1}(-\infty, x - 2^{-n}]$$

Es decir

$$f^{-1}(-\infty, x) \subset \bigcup_{n=1}^{\infty} f^{-1}(-\infty, x - 2^{-n}] \qquad (4)$$

Las inclusiones (3) y (4) demuestran la igualdad propuesta.

### 4.10. RESTRICCION Y EXTENSION DE UNA FUNCION

Sean $f: X \to Y$ y A un subconjunto de X. Definimos la función $g: A \to Y$ mediante la asignación $g(x) = f(x)$ cualquiera que sea $x \in A$. Decimos que $g$ es la restricción de la aplicación $f$ al subconjunto A, y la denotamos $g = f \mid A$.

Si $g$ es la restricción de $f$ al subconjunto A, entonces $f: X \to Y$ es una extensión de la función $g$ sobre el conjunto X. Es claro que la restricción de $f: X \to Y$ al subconjunto A es única; mientras que, dada una función $g: A \to Y$, ésta admite más de una extensión sobre el conjunto X que contiene a A. En efecto, si $g: A \to Y$ y $A \subset X$, entonces podemos definir una extensión de $g$ al conjunto X, de la siguiente manera, sea $y_0$ un elemento cualquiera de Y; definimos:

$$f: X \to Y \text{ mediante } f(x) = \begin{cases} g(x) & \text{si } x \in A \\ y_0 & \text{si } x \in X - A \end{cases}$$

## TRABAJO PRACTICO IV

*4-25.* Dados $A = \{1, 2, 3\}$ y $B = \{0, 1, 2, 3, 8\}$ definir por extensión la función $f: A \to B$, que asigna a cada elemento del dominio su cuadrado disminuido en 1. Representar y clasificar $f$.

*4-26.* Siendo $A = \{-2, -1, 1, 3\}$ representar y clasificar la aplicación $f: A \to \mathbf{Z}$, tal que la imagen de cada elemento de A es el resto de su división por 3.

*4-27.* Por definición, parte entera de un número real $x$ es el mayor entero que no supera a $x$. Si $e$ es la parte entera de $x$ se verifica

$$e \leqslant x < e + 1$$

Para denotar la parte entera del número real $x$, se usan las notaciones ent $(x)$ o $[x]$.

Estudiar, representar y clasificar la función $f: \mathbf{R} \to \mathbf{Z}$, definida por

$$f(x) = \text{ent}\,(x)$$

*4-28.* Representar y clasificar la función mantisa, que se denota por

$$\text{mant}: \mathbf{R} \to \mathbf{R}$$

y se define mediante mant $(x) = x - \text{ent}\,(x)$

4-29. Representar y clasificar las siguientes funciones:

i ) $f: \mathbf{R} \to \mathbf{R}$ tal que $f(x) = x - 1$

ii ) $f: \mathbf{R} \to [1, \infty)$ tal que $f(x) = x^2 + 1$

iii) $f: \mathbf{Z} \to \mathbf{Q}$ definida por $f(x) = \dfrac{x-1}{2}$

*4-30.* Sean $A = \{1, 2, 3\}$ y $B = \{2, 3\}$

Representar y clasificar $f: A \times B \to \mathbf{Z}$ definida por

$$f(a, b) = 3a - b$$

*4-31.* Dados $A = \{1, 2, 3\}$ y $B = \{1, 2, 3, 4\}$ definir por una tabla y clasificar

$$f: P(A) \to P(B) \quad \text{tal que} \quad f(X) = B - X$$

*4-32.* Definir aplicaciones no constantes, con los dominios y codominios que se indican:

i ) $f : \mathbf{Q} \to \mathbf{Z}$

ii ) $g : \mathbf{Z} \to \mathbf{N}$ (que sea biyectiva)

iii) $h : \mathbf{R} \to \{0, 1\}$

*4-33.* Sean $f : \mathbf{Z} \to \mathbf{N}$ definida por $f(x) = x^2$, y los subconjuntos del dominio $A = \{-1, -2, -3, 4\}$ y $B = \{1, 2, 3, 4\}$

Verificar las propiedades de la imagen.

*4-34.* Se considera la función $f : \mathbf{R}^2 \to \mathbf{R}$ tal que $f(x, y) = y$.
Dar dos subconjuntos A y B del dominio, tales que $B \subset A$ y $f(A - B) \neq \neq f(A) - f(B)$

*4-35.* Proponer dos conjuntos X e Y, una parte $A \subset X$ y una función $f : X \to Y$ tales que

i ) $f(X - A) \subset Y - f(A)$

ii ) $Y - f(A) \subset f(X - A)$

iii) $f(X - A) \cap [Y - f(A)] = \phi$

*4-36.* Sea $f : \mathbf{R} \to \mathbf{R}$ definida por $f(x) = x^2 + 1$. Determinar las preimágenes de los siguientes subconjuntos del codominio:

$$[-1, 1), (-\infty, \frac{1}{2}], [0, 3], [0, 3), [1, 10]$$

*4-37.* Sea $f : X \to Y$. Demostrar la equivalencia de las siguientes proposiciones:

a) $f$ es inyectiva.

b) $\forall A, A \subset X \Rightarrow f^{-1}[f(A)] = A$

*4-38.* Las funciones $f : \mathbf{Z} \to \mathbf{Q}$ y $g : \mathbf{Q} \to \mathbf{Z}$ son tales que

$$f(x) = \frac{x^2}{2} + 1 \quad \text{y} \quad g(x) = \text{ent}(x)$$

Definir $g \circ f$, $f \circ g$, y determinar $(g \circ f)(-2)$, $(f \circ g)(-\frac{1}{2})$.

*4-39.* Las funciones $f : A \to B$ y $g : B \to C$ son tales que $g \circ f$ es sobreyectiva. Demostrar que $g$ es sobreyectiva.

*4-40.* Las funciones $f : A \to B$, $g : B \to C$ y $h : C \to D$ son tales que $g \circ f$ y $h \circ g$ son biyectivas. Demostrar que $f$, $g$ y $h$ son biyectivas.

*4-41.* Las funciones $f : A \to B$, $g : B \to C$ y $h : C \to A$ son tales que $h \circ g \circ f$ y $f \circ h \circ g$ son sobreyectivas, mientras que $g \circ f \circ h$ es inyectiva. Demostrar que $f$, $g$ y $h$ son biyectivas.

**4-42.** Sean $f : X \to Y$ una función, y los subconjuntos $A \subset X$ y $B \subset Y$. Demostrar las siguientes relaciones:

a) $A \subset f^{-1}[f(A)]$

b) $f[f^{-1}(B)] \subset B$

c) $f(X) - f(A) \subset f(X - A)$

d) $f^{-1}(Y - B) = X - f^{-1}(B)$

e) $f(A \cap f^{-1}(B)) = f(A) \cap B$

**4-43.** Dado el subconjunto $A \subset X$ definimos la aplicación

$$\chi_A : X \to \mathbf{R} \text{ mediante}$$

$$\chi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \in X - A \end{cases}$$

$\chi_A$ se llama función característica del subconjunto $A \subset X$.
Verificar que para todo elemento $x$ de un conjunto X se cumplen las siguientes relaciones entre las funciones características de los subconjuntos de X:

i) $\chi_{A \cap B}(x) = \chi_A(x)\, \chi_B(x)$

ii) $\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$

**4-44.** Se considera la función $f : X^2 \to X^2$ definida por $f(a, b) = (b, a)$
Demostrar que $f \circ d = d$, siendo $d : X \to X^2$ la función diagonal.

**4-45.** La función $f : \mathbf{R} \to \mathbf{R}^2$ está definida por $f(x) = (x, -x)$. Demostrar:

i) $f(x + y) = f(x) + f(y)$

ii) $f(k \cdot x) = k \cdot f(x)$, donde $k \in \mathbf{R}$

Nota: las condiciones i) y ii) confieren a $f$ el carácter de función lineal.

**4-46.** Sea $f$ una función arbitraria de un conjunto A en **R**. Demostrar que para todo número real $x$ se verifica

$$\bigcap_{n=1}^{\infty} f^{-1}(-\infty, x + 2^{-n}) = f^{-1}(-\infty, x]$$

**4-47.** Sea $A$ es un álgebra de Boole de subconjuntos de $\Omega$, y P es una función de $A$ en **R** que satisface:

i) $P(A) \geqslant 0$ cualquiera que sea A

ii) $P(\Omega) = 1$

iii) $P\left(\sum_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i)$

La aplicación P, que verifica las condiciones anteriores, se llama función de probabilidad; los elementos del dominio son sucesos, y la imagen de cada uno de ellos es su probabilidad.
Demostrar:

a) La probabilidad del vacío es igual a 0.

b) La probabilidad de la unión de dos sucesos es igual a la suma de sus probabilidades menos la probabilidad de su intersección.

c) La probabilidad del complemento de un suceso es igual a 1 menos la probabilidad de dicho suceso.

*4-48.* Sean un álgebra de sucesos de $\Omega$ y X una función de $\Omega$ en **R**. Demostrar que para todo $x \in \mathbf{R}$

$$X^{-1}(-\infty, x) \in A \Leftrightarrow X^{-1}(-\infty, x] \in A$$

*4-49.* En las mismas condiciones del ejercicio anterior demostrar

$$X^{-1}(-\infty, x] \in A \Leftrightarrow X^{-1}[x, \infty) \in A$$

*4-50.* En el mismo caso, demostrar

$$X^{-1}(-\infty, x] \in A \Leftrightarrow X^{-1}(x, \infty) \in A$$

*4-51.* Sea $f: X \to Y$. Demostrar la equivalencia de las siguientes proposiciones cualesquiera que sean $A \subset X$ y $B \subset X$

i ) $f^{-1}[f(A)] = A$

ii ) $f(A \cap B) = f(A) \cap f(B)$

iii) $A \cap B = \phi \Rightarrow f(A) \cap f(B) = \phi$

iv) $B \subset A \Rightarrow f(A - B) = f(A) - f(B)$

Capítulo 5

# LEYES DE COMPOSICION

## 5.1. INTRODUCCION

En este capítulo definimos, desde el punto de vista funcional, el concepto de ley de composición interna en un conjunto no vacío. Luego de proponer algunos ejemplos, se estudian las posibles propiedades que pueden presentarse y la eventual existencia de elementos distinguidos. Se introduce aquí el tema de homomorfismo entre conjuntos, y su culminación en el teorema fundamental de compatibilidad de una relación de equivalencia con una ley interna. Con vistas a su utilización en la estructura de espacio vectorial, se definen las leyes de composición externa.

## 5.2. LEYES DE COMPOSICION INTERNA

Una ley de composición interna, definida en un conjunto no vacío A, consiste en una operación que asigna a cada par ordenado de elementos de A un único elemento de A. Esto significa que a cada objeto de A X A le corresponde un único elemento de A.

***Definición***

Ley de composición interna definida en un conjunto no vacío A, es toda función de A X A en A.

En símbolos

$$* \text{ es una ley interna en A} \Leftrightarrow * : A^2 \rightarrow A$$

Es decir

$$a \in A \;\wedge\; b \in A \Rightarrow a * b \in A$$

La unicidad de $a * b$ está dada por la definición de función. La imagen $a * b$, del par $(a ; b)$, es el compuesto de $a$ con $b$.

Son ejemplos de leyes de composición interna, la adición y multiplicación en **N**, **Z**, **Q**, **R** y **C**.

***Ejemplo 5-1.***

Las siguientes tablas de doble entrada definen leyes de composición interna en el conjunto $A = \{a, b, c\}$

i)

| $*$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $a$ | $b$ |

ii)

| $*$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $b$ |
| $b$ | $c$ | $a$ | $c$ |
| $c$ | $b$ | $c$ | $a$ |

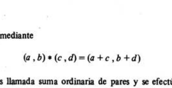
En i ) es $b * c = a$, pero en ii ) se tiene $b * c = c$. ¿Cuántas leyes de composición interna es posible definir en este conjunto A? Es obvio que tantas como funciones existan de $A^2$ en A; como $A^2$ tiene 9 elementos, se trata de todas las variaciones con repetición de 3 elementos de orden 9, es decir, $3^9$.

***Ejemplo 5-2.***

En $\mathbf{R}^2$ se define $*$ mediante

$$(a, b) * (c, d) = (a + c, b + d)$$

Esta ley interna es llamada suma ordinaria de pares y se efectúa sumando en **R**, componente a componente. Como cada par ordenado de números reales caracteriza un vector del plano aplicado en el origen de un sistema cartesiano, resulta que el significado geométrico de esta ley de composición interna en $\mathbf{R}^2$ consiste en la diagonal del paralelogramo cuyos lados son los vectores dados.



*Ejemplo 5-3.*

Dado $A = \{1, 2, 3\}$ se considera el conjunto T(A) cuyos elementos son todas las funciones biyectivas de A en A, es decir

$$T(A) = \{f_i : A \to A \,/\, f_i \text{ es biyectiva}\}$$

Nos interesa definir en T(A) la composición de aplicaciones, que es obviamente una ley de composición interna, puesto que la composición de aplicaciones biyectivas de A en A conduce a aplicaciones biyectivas de A en A.

El conjunto T(A) tiene 6 elementos, que caracterizamos a través de los correspondientes conjuntos imágenes de las aplicaciones

$$f_1 = \{(1,1),(2,2),(3,3)\} = i_A \qquad f_4 = \{(1,2),(2,3),(3,1)\}$$

$$f_2 = \{(1,1),(2,3),(3,2)\} \qquad f_5 = \{(1,3),(2,1),(3,2)\}$$

$$f_3 = \{(1,2),(2,1),(3,3)\} \qquad f_6 = \{(1,3),(2,2),(3,1)\}$$

Para componer $f_2$ con $f_3$ determinamos $f_3 \circ f_2$ mediante:

$$(f_3 \circ f_2)(1) = f_3\,[f_2\,(1)] = f_3\,(1) = 2$$
$$(f_3 \circ f_2)(2) = f_3\,[f_2\,(2)] = f_3\,(3) = 3$$
$$(f_3 \circ f_2)(3) = 1$$

Resulta así $f_3 \circ f_2 = f_4$.

El lector puede completar la tabla de la composición de las funciones biyectivas de A en A, como en el caso del ejemplo 5-1.

## 5.3. PROPIEDADES Y ELEMENTOS DISTINGUIDOS DE LAS LEYES DE COMPOSICION INTERNA

Sea $*$ una ley de composición interna en A, es decir, $* : A^2 \to A$

### 5.3.1. Asociatividad

$* : A^2 \to A$ es asociativa $\Leftrightarrow (a * b) * c = a * (b * c)$ cualesquiera que sean $a$, $b$ y $c$ en A.

### 5.3.2. Conmutatividad

$* : A^2 \to A$ es conmutativa $\Leftrightarrow a * b = b * a$ para todo par de elementos $a$ y $b$ de A.

### 5.3.3. Existencia de elemento neutro

Cabe preguntarse si existe en el conjunto A un elemento $e$, que compuesto a izquierda y a derecha con cualquiera otro no lo altere. Si un elemento tal existe se lo llama neutro o identidad respecto de la ley $*$ de acuerdo con la siguiente definición

$$e \in A \text{ es neutro respecto de } * \Leftrightarrow \forall a \in A : a * e = e * a = a$$

### 5.3.4. Existencia de inversos en una ley con neutro

Sea $*$ una ley interna en A, con elemento neutro $e$. Dado $a \in A$ interesa investigar si existe $a' \in A$, tal que compuesto a izquierda y a derecha con $a$ dé por resultado $e$. El neutro es un elemento del conjunto relativo a todos. El inverso, si existe, es relativo a cada elemento. Proponemos la siguiente definición

$$a' \in A \text{ es inverso de } a \in A \text{ respecto de } * \Leftrightarrow a * a' = a' * a = e$$

Los elementos de A que admiten inversos respecto de $*$ se llaman inversibles.

*Ejemplo 5-4.*

i ) La adición es una ley interna en **N**, conmutativa y asociativa.

ii ) La adición es ley interna en **Z**, asociativa, conmutativa, con neutro 0, y con inverso aditivo para cada entero.

iii) En **R** la multiplicación es ley interna, asociativa, conmutativa, con neutro 1, y con inverso multiplicativo para cada elemento no nulo.

iv) En el conjunto T(A) del ejemplo 5-3, la composición de aplicaciones es ley interna, asociativa (la composición de funciones es asociativa), con neutro $f_1 = i_A$, y con inverso para cada elemento. Estas propiedades son verificables sencillamente mediante la tabla de la composición.

### 5.3.5. Unicidad del neutro

Si existe neutro en A respecto de $*$, entonces es único.

Supongamos que $e$ y $e'$ son neutros respecto de $*$; entonces, por ser $e$ neutro y por serlo $e'$, se tiene

$$e' = e' * e = e * e' = e$$

### 5.3.6. Unicidad del inverso respecto de una ley asociativa

Si un elemento $a \in A$ admite inverso respecto de la ley asociativa $*$, entonces dicho inverso es único.

Supongamos que $a'$ y $a''$ son inversos de $a$. Aplicando consecutivamente la defini-

ción de neutro, el hecho de que $a'$ es inverso de $a$, la asociatividad, el supuesto de que $a''$ es inverso de $a$, y la definición de neutro se tiene

$$a'' = a'' * e = a'' * (a * a') = (a'' * a) * a' = e \ * a' = a'$$

### 5.3.7. Regularidad de un elemento respecto de una ley interna

La regularidad de un elemento respecto de una ley de composición interna consiste en que es cancelable o simplificable a izquierda y a derecha en los dos miembros de una igualdad.

***Definición***

$$a \in A \text{ es regular respecto de } * \Leftrightarrow \begin{cases} a * b = a * c \Rightarrow b = c \\ b * a = c * a \Rightarrow b = c \end{cases}$$

La regularidad bilateral se llama regularidad a secas; si es preciso distinguir, habrá que especificar si lo es a izquierda o a derecha.

La regularidad es relativa a la ley de composición, y, lo mismo que la inversión, depende de cada elemento. Así como existen elementos que admiten inverso, y otros que no, aquí puede ocurrir que un elemento sea regular o no. Si todos los elementos de un conjunto son regulares respecto de cierta ley de composición interna, se dice que vale la ley cancelativa o de simplificación.

***Ejemplo 5-5.***

i ) En $(\mathbf{Z}, +)$ todos los enteros son regulares.

ii ) En $(\mathbf{N}, .)$ todos los naturales son regulares.

iii) En $(\mathbf{R}, .)$ todos los reales, salvo el cero, son regulares.

iv) En $(\mathbf{R}^2, +)$ todos los elementos son regulares. En este ejemplo de ley de composición interna valen la asociatividad, conmutatividad, existe neutro $(0, 0)$ y el inverso aditivo u opuesto de todo par $(a, b)$ es $(-a, -b)$.

***Ejemplo 5-6.***

Se define $* : \mathbf{Q}^2 \to \mathbf{Q}$ mediante $a * b = a + b + a \, . \, b$ (1)

Se entiende que + y . son la suma y el producto ordinarios de racionales, de modo que (1) caracteriza una ley de composición interna en **Q**.

El problema consiste en analizar las propiedades de * en **Q**.

i ) Asociatividad. Aplicando reiteradamente la definición (1)

$$(a * b) * c = (a + b + a \, . \, b) * c = a + b + a \, . \, b + c + (a + b + a \, . \, b) \, . \, c =$$
$$= a + b + c + ab + ac + bc + abc \qquad (2)$$
$$a * (b * c) = a * (b + c + b \, . \, c) = a + b + c + b \, . \, c + a \, . \, (b + c + b \, . \, c) =$$
$$= a + b + c + ab + ac + bc + abc \qquad (3)$$

De (2) y (3) resulta $(a * b) * c = a * (b * c)$ y la ley es asociativa.

ii ) Conmutatividad. Se verifica aplicando (1) y la conmutatividad de la adición y multiplicación en **Q**

$$a * b = a + b + a \cdot b = b + a + b \cdot a = b * a$$

iii) Existencia de neutro. Si existe $e$, para todo $a \in \mathbf{Q}$ debe cumplirse

$$a * e = a$$

Por (1) $\quad a + e + a \cdot e = a$ , es decir : $e + a \cdot e = 0$ .

Luego $(1 + a) \cdot e = 0$ y cualquiera que sea $a \neq -1$, resulta $e = 0$.

Si $a = -1$, se tiene $a * e = (-1) * 0 = -1 + 0 + (-1) \cdot 0 = -1$

Resulta entonces que existe $e = 0$. Por la conmutatividad, sólo hemos analizado con $e$ a derecha.

iv) Elementos de **Q** que admiten inverso respecto de $*$. Si $a \in \mathbf{Q}$ admite inverso, debe existir $a' \in \mathbf{Q}$, tal que

$$a * a' = e$$

es decir $\quad a + a' + a \cdot a' = 0 \Rightarrow a' \cdot (1 + a) = -a$ .

Luego, si $a \neq -1$, existe $a' = \dfrac{-a}{1 + a}$

Es decir, todos los racionales, salvo $-1$, admiten inverso respecto de $*$.

v ) Elementos regulares. Investigamos qué racionales $a$ son regulares a izquierda. Sea entonces

$$a * b = a * c$$

Por (1)

$$a + b + a \cdot b = a + c + a \cdot c$$

Cancelando $a$ en $(\mathbf{Q}, +)$ tenemos

$$b + a \cdot b = c + a \cdot c$$

Por distributividad

$$b\,(1 + a) = c\,(1 + a)$$

Si $a \neq -1$, entonces

$$b = c$$

Luego, todos los racionales, salvo $-1$, son regulares respecto de $*$. O bien, vale la ley cancelativa de $*$ para todo racional distinto de $-1$.

***Ejemplo 5-7.***

Se considera el par (A , .) siendo "." el producto ordinario de números reales, y A el subconjunto de números reales del tipo $a + b\sqrt{2}$ con $a$ y $b$ racionales. Estamos interesados en caracterizar las propiedades de esta ley de composición en A.

i ) El producto es ley interna en A, o equivalentemente, A es cerrado para el producto. En efecto, sean

$$\alpha = a + b\sqrt{2} \in A \ \wedge \ \beta = c + d\sqrt{2} \in A \Rightarrow$$
$$\Rightarrow \alpha \,.\, \beta = (a + b\sqrt{2})\,.\,(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

y como $a, b, c, d \in \mathbf{Q}$, resulta $\alpha \,.\, \beta \in A$.

ii ) El producto en A es asociativo, por ser A un subconjunto de **R**, donde se sabe que la multiplicación es ley asociativa. Debe quedar claro que las igualdades que se verifican para todos los elementos de un conjunto se siguen cumpliendo en cualquier subconjunto de él. Sólo es preciso probar las propiedades relativas a la existencia.

iii) Por las razones expuestas en ii ), el producto en A es conmutativo

$$\forall \alpha \ \forall \beta \in A : \alpha \,.\, \beta = \beta \,.\, \alpha$$

iv) Neutro es $e = 1 + 0 \,.\, \sqrt{2}$, pues

$$(a + b\sqrt{2})(1 + 0\sqrt{2}) = a + b\sqrt{2}$$

O bien, si existe neutro en A debe ser del tipo $e = x + y\sqrt{2}$, tal que para todo $\alpha = a + b\sqrt{2}$ debe cumplirse

$$(a + b\sqrt{2})\,.\,(x + y\sqrt{2}) = a + b\sqrt{2} \qquad (1)$$

con $x$ e $y$ a determinar. Efectuando operaciones:

$$(ax + 2by) + (bx + ay)\sqrt{2} = a + b\sqrt{2}$$

$$(2) \begin{cases} ax + 2by = a \\ bx + \ \ ay = b \end{cases}$$

Si $a = b = 0$ (1) se cumple obviamente. Supongamos entonces que $a$ y $b$ no son simultáneamente nulos y utilicemos el método de Crámer para resolver (2)

$$\Delta = \begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = a^2 - 2b^2 \neq 0 \qquad \text{pues } a \text{ y } b$$

son enteros no simultáneamente nulos por lo supuesto.

$$\Delta x = \begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = a^2 - 2b^2$$

$$\Delta y = \begin{vmatrix} a & a \\ b & b \end{vmatrix} = ab - ab = 0$$

Entonces

$$x = \frac{\Delta x}{\Delta} = 1 \quad , \quad y = \frac{\Delta y}{\Delta} = 0$$

Es decir, existe $e = 1 + 0\sqrt{2}$

v) Todo real no nulo admite inverso multiplicativo. Se trata de ver aquí que si $\alpha = a + b\sqrt{2} \neq 0 + 0 . \sqrt{2}$, entonces su recíproco pertenece a A. Si existe será del tipo $x + y\sqrt{2}$ tal que

$$(x + y\sqrt{2}) . (a + b\sqrt{2}) = 1 + 0\sqrt{2}$$

$$\Downarrow$$

$$(ax + 2\,by) + (bx + ay)\sqrt{2} = 1 + 0\sqrt{2}$$

$$\Downarrow$$

$$\begin{cases} ax + 2\,by = 1 \\ bx + ay = 0 \end{cases}$$

$$\Downarrow$$

$$\Delta = a^2 - 2\,b^2 \neq 0 \quad , \quad \Delta x = \begin{vmatrix} 1 & 2b \\ 0 & a \end{vmatrix} = a \; , \; \Delta y = \begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix} = -b$$

Es decir $\quad x = \dfrac{a}{a^2 - 2\,b^2} \; , \; y = \dfrac{-b}{a^2 - 2\,b^2}$

y resulta $\quad \alpha^{-1} = \dfrac{a}{a^2 - 2\,b^2} - \dfrac{b}{a^2 - 2\,b^2}\sqrt{2}$

vi) En cuanto a la ley de simplificación, todo elemento no nulo de A es regular, pues si $\alpha \neq 0$ y $\alpha\,\beta = \alpha\,\gamma$ , entonces

$$\alpha\beta - \alpha\gamma = 0$$

$$\Rightarrow \alpha(\beta - \gamma) = 0$$

$$\Rightarrow \beta - \gamma = 0 \Rightarrow \beta = \gamma$$

***Ejemplo 5-8.***

Sea $\mathbf{R}^{n \times m}$ el conjunto de las matrices reales de $n$ filas y $m$ columnas.
Definimos la adición de matrices en $\mathbf{R}^{n \times m}$ mediante

$$A + B = [a_{ij}] + [b_{ij}] = C \text{ tal que } c_{ij} = a_{ij} + b_{ij} \;\; \forall i \, \forall j$$

Es decir, dos matrices $n \times m$ se suman elemento a elemento. Resulta claro que esta definición caracteriza una ley de composición interna en $\mathbf{R}^{n \times m}$, que verifica las siguientes propiedades:

i ) Asociatividad. Basándonos en la asociatividad de la adición en R

$$(A + B) + C = ([a_{ij}] + [b_{ij}]) + [c_{ij}] =$$

$$= [a_{ij} + b_{ij}] + [c_{ij}] = [(a_{ij} + b_{ij}) + c_{ij}] =$$

$$= [a_{ij} + (b_{ij} + c_{ij})] = [a_{ij}] + [b_{ij} + c_{ij}] =$$

$$= [a_{ij}] + ([b_{ij}] + [c_{ij}]) = A + (B + C)$$

ii ). Conmutatividad. Con el mismo criterio anterior.

$$A + B = [a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}] =$$
$$= [b_{ij} + a_{ij}] = [b_{ij}] + [a_{ij}] = B + A$$

Hemos utilizado, sucesivamente, la definición de adición de matrices, la conmutatividad de la suma en R, y nuevamente la definición de adición de matrices.

iii) Elemento neutro es la matriz nula $N \in R^{n \times m}$ definida por $n_{ij} = 0$, $\forall i\ \forall j$, pues cualquiera que sea A en dicho conjunto

$$A + N = N + A = A$$

iv) Inversa aditiva de toda matriz $A \in R^{n \times m}$ es la matriz $B \in R^{n \times m}$ definida por $b_{ij} = -a_{ij}\ \forall (i\,;j)$, pues

$$A + B = B + A = N$$

La matriz B, inversa aditiva de A, se llama opuesta de A, y se denota por $-A$

v ) Toda matriz $n \times m$ es regular respecto de la adición. En efecto

$$A + B = A + C \text{ , y sumando } -A$$
$$-A + (A + B) = -A + (A + C)$$

asociando $(-A + A) + B = (-A + A) + C$

por iv) $N + B = N + C$

y por iii) $B = C$

### 5.3.8. Distributividad de una ley de composición interna respecto de otra

Consideremos el caso de dos leyes de composición interna "$*$" y "$\circ$", definidas en un mismo conjunto A. Interesa caracterizar el comportamiento relativo de dichas leyes internas en el sentido de obtener elementos del tipo $(a * b) \circ c$, o bien $(a \circ b) * c$.

***Definición***

"$\circ$" es distributiva a derecha respecto de "$*$" si y sólo si

$$(a * b) \circ c = (a \circ c) * (b \circ c)$$

para toda terna de elementos $a$, $b$ y $c$ en A.

La distributividad a izquierda de "$\circ$" respecto de "$*$" queda definida por

$$a\,,b\,,c \in A \Rightarrow c \circ (a * b) = (c \circ a) * (c \circ b)$$

Se dice que "$\circ$" es distributiva respecto de $*$ si y sólo si lo es a izquierda y a derecha.

Análogamente se define la distributividad de "$*$" respecto de "$\circ$".

***Ejemplo 5-9.***

i ) La adición y multiplicación son leyes de composición interna en **R**, y la segunda es distributiva respecto de la primera. Pero la adición no lo es respecto de la multiplicación.

ii ) En el conjunto **N** la potenciación no es distributiva respecto de la adición. Aquí se define

$$a * b = a^n \text{ y se tiene } (a+b)^n \neq a^n + b^n .$$

Tampoco existe distributividad a izquierda, pues

$$n^{(a+b)} \neq n^a + n^b$$

iii) Pero la potenciación en **N** es distributiva a derecha, respecto de la multiplicación, ya que

$$(a \,.\, b)^n = a^n \,.\, b^n$$

Sin embargo, no lo es a izquierda, pues

$$n^{(a.\,b)} \neq n^a \,.\, n^b$$

iv) En $P$ (U) la unión e intersección son leyes de composición interna, y cada una es distributiva respecto de la otra.

v ) En $P$(U) se consideran la diferencia simétrica y la intersección. En el ejemplo 2-28 se ha probado la distributividad de la intersección respecto de aquélla.

## 5.4. HOMOMORFISMOS ENTRE CONJUNTOS

Sean (**R**, +) y ($\mathbf{R}^+$, . ), donde **R** es el conjunto de los reales, $\mathbf{R}^+$ el conjunto de los reales positivos y las operaciones indicadas son la suma y el producto usuales.

Consideremos ahora la función

$$f : \mathbf{R} \to \mathbf{R}^+$$

definida por $f(x) = 2^x$ (1).

Se tiene entonces

$$f(x+y) = 2^{x+y} = 2^x \,.\, 2^y = f(x) \,.\, f(y)$$

Basándonos en la definición (1), el producto de potencias de igual base, y utilizando de nuevo la definición (1), hemos probado que la imagen de la suma en **R** es igual al producto de las imágenes en $\mathbf{R}^+$.

Una aplicación $f$, que satisface esta propiedad, se dice un homomorfismo de **R** en $\mathbf{R}^+$ respecto de las correspondientes leyes de composición interna.

### 5.4.1. Homomorfismo entre dos conjuntos respecto de una ley interna en cada uno

Sean los conjuntos no vacíos A, A', y las leyes de composición interna

$$* : A^2 \to A$$
$$*' : A'^2 \to A'$$

***Definición***

La función $f : A \to A'$ es un homomorfismo respecto de $*$ y $*'$ si y sólo si la imagen de la composición en A es igual a la composición de las imágenes en A'.

En símbolos

$f : A \to A'$ es homomorfismo respecto de $*$ y $*'$ $\Leftrightarrow f(a * b) = f(a) *' f(b)$

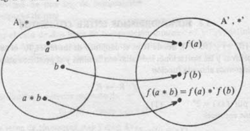
cualesquiera que sean $a$ y $b$ en A.

El concepto de homomorfismo es fundamental en álgebra, y su interpretación es la siguiente:

i ) Hemos definido homomorfismo entre dos conjuntos respecto de sendas leyes de composición interna. Las leyes internas y los conjuntos no son necesariamente distintos. Además, el concepto de homomorfismo es aplicable también respecto de relaciones que no son necesariamente operaciones. Se tienen, por ejemplo, los homomorfismos de orden.

ii ) Un homomorfismo, como objeto, es una función que respecta la propiedad que lo define.

iii) El homomorfismo $f : A \to A'$ proporciona una alternativa para obtener la imagen de la composición en A, a saber:




a) $a \in A \ \wedge \ b \in A \Rightarrow a * b \in A \Rightarrow$
$\Rightarrow f(a * b) \in A'$

b) $a \in A \ \wedge \ b \in A \Rightarrow f(a) \in A' \ \wedge \ f(b) \in A' \Rightarrow$
$\Rightarrow f(a) *' f(b) \in A'$

El homomorfismo establece la igualdad de los objetos $f(a * b)$ y $f(a) *' f(b)$, y las dos posibilidades son: componer en A y hallar la imagen, o bien, hallar cada imagen y componer éstas en A'. Como sinónimo suele utilizarse el vocablo morfismo.

### 5.4.2. Homomorfismos especiales

Sea $f: A \to A'$ un homomorfismo respecto de $*$ y $*'$.

i ) $f$ es un monomorfismo si y sólo si $f$ es inyectiva.

ii ) $f$ es un epimorfismo si y sólo si $f$ es sobreyectiva.

iii) $f$ es un isomorfismo si y sólo si $f$ es biyectiva.

iv) $f$ es un endomorfismo si y sólo si $A = A'$.

v ) $f$ es un automorfismo si y sólo si $f$ es un endomorfismo biyectivo.

*Ejemplo 5-10.*

Sean $(\mathbf{R}^3, +)$, $(\mathbf{R}^{2\times 2}, +)$ y $f: \mathbf{R}^3 \to \mathbf{R}^{2\times 2}$ tal que

$$f(x_1, x_2, x_3) = \begin{bmatrix} x_1 & 0 \\ x_2 & x_3 \end{bmatrix}$$

Las operaciones consideradas son la suma de ternas ordenadas de números reales definida por

$$(x_1, x_2, x_3) + (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$$

y la adición en $\mathbf{R}^{2\times 2}$ es la definida en el ejemplo 5-8. Vamos a probar que $f$ caracteriza un homomorfismo.

Sea

$$f[(x_1, x_2, x_3) + (y_1, y_2, y_3)] = f(x_1 + y_1, x_2 + y_2, x_3 + y_3) =$$

$$= \begin{bmatrix} x_1 + y_1 & 0 \\ x_2 + y_2 & x_3 + y_3 \end{bmatrix} = \begin{bmatrix} x_1 & 0 \\ x_2 & x_3 \end{bmatrix} + \begin{bmatrix} y_1 & 0 \\ y_2 & y_3 \end{bmatrix} = f(x_1, x_2, x_3) + f(y_1, y_2, y_3)$$

Además $f$ es un monomorfismo, es decir, inyectiva. En efecto, sean

$$(x_1, x_2, x_3) \in \mathbf{R}^3 \wedge (y_1, y_2, y_3) \in \mathbf{R}^3 \,/\, f(x_1, x_2, x_3) = f(y_1, y_2, y_3) \Rightarrow$$

$$\Rightarrow \begin{bmatrix} x_1 & 0 \\ x_2 & x_3 \end{bmatrix} = \begin{bmatrix} y_1 & 0 \\ y_2 & y_3 \end{bmatrix} \Rightarrow x_1 = y_1 \, , \, x_2 = y_2 \, , \, x_3 = y_3 \Rightarrow$$

$$\Rightarrow (x_1, x_2, x_3) = (y_1, y_2, y_3)$$

En cambio $f$ no es sobreyectiva, pues $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ carece de preimagen.

*Ejemplo 5-11.*

Sea $f: \mathbf{R} \to \mathbf{R}$ tal que $f(x) = -3x$.

Resulta $f$ un automorfismo de $\mathbf{R}$ en sí mismo, respecto de la adición, pues

i) $f(a+b) = -3 \cdot (a+b) = -3a - 3b = f(a) + f(b)$

ii) $f$ es biyectiva, lo que se prueba siguiendo el esquema del ejemplo 4-9.

El lector podrá comprobar fácilmente que $f: \mathbf{R} \to \mathbf{R}$ definida por $f(x) = x + 1$, no es un homomorfismo respecto de la adición.

## 5.5. COMPATIBILIDAD DE UNA RELACION DE EQUIVALENCIA CON UNA LEY INTERNA

Sean $A \neq \phi$, $\sim$ una relación de equivalencia definida en A, y $*$ una ley de composición interna en A. Cabe preguntarse si la composición de pares de elementos respectivamente equivalentes conduce a resultados equivalentes. Si la respuesta es afirmativa, se dice que la relación de equivalencia es compatible con la ley de composición interna.

***Definición***

$\sim$ es compatible con $* \Leftrightarrow a \sim a' \wedge b \sim b' \Rightarrow a * b \sim a' * b'$ cualesquiera que sean $a$, $b$, $a'$ y $b'$ en A.

*Ejemplo 5-12.*

Investigamos la compatibilidad de la congruencia módulo $n$, respecto de la adición en Z.

$$\text{Sean } a \sim a' \wedge b \sim b' \Rightarrow n \mid a - a' \wedge n \mid b - b' \Rightarrow n \mid (a - a') + (b - b') \Rightarrow$$
$$\Rightarrow n \mid (a + b) - (a' + b') \Rightarrow a + b \sim a' + b'$$

Hemos utilizado sucesivamente la definición de la congruencia módulo $n$, el hecho de que si un número es divisor de otros dos es divisor de su suma, suma de dos diferencias, y finalmente la definición de la misma relación de equivalencia.

*Ejemplo 5-13.*

De manera semejante comprobamos la compatibilidad de la congruencia módulo $n$, respecto de la multiplicación en Z.

$$a \sim a' \wedge b \sim b' \Rightarrow n \mid a - a' \wedge n \mid b - b' \Rightarrow a = a' + nk' \wedge b = b' + nk'' \Rightarrow$$
$$\Rightarrow ab = a'b' + a'nk'' + nk'b' + nk'nk'' \Rightarrow ab = a'b' + n(a'k'' + k'b' + k'nk'')$$
$$\Rightarrow ab = a'b' + nk \Rightarrow ab - a'b' = nk \Rightarrow n \mid ab - a'b' \Rightarrow ab \sim a'b'$$

***Ejemplo 5-14.***

En el conjunto $N^2$ de todos los pares ordenados de números naturales se considera la relación de equivalencia estudiada en el ejercicio 3-25, y la suma ordinaria de pares, definida por

$$(a\,,b)+(c\,,d)=(a+c,\ b+d) \qquad (1)$$

Sean $(a\,,b)\sim(a'\,,b') \ \wedge\ (c\,,d)\sim(c'\,,d') \Rightarrow a+b'=b+a' \ \wedge\ c+d'=d+c' \Rightarrow$
$\Rightarrow (a+c)+(b'+d')=(b+d)+(a'+c') \Rightarrow (a+c\,,b+d)\sim(a'+c'\,,b'+d') \Rightarrow$
$\Rightarrow (a\,,b)+(c\,,d)\sim(a'b')+(c'\,,d')$

De este modo resulta que la relación de equivalencia definida en $N^2$ es compatible con la adición definida en (1).

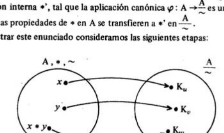
### 5.5.1. Teorema fundamental de compatibilidad

El hecho de que una relación de equivalencia sea compatible con una ley de composición interna definida en un conjunto es de notable importancia, porque induce una ley de composición interna en el conjunto cociente, es decir, permite operar con clases de equivalencia.

**Teorema**

Si $\sim$ es una relación de equivalencia compatible con la ley de composición interna $*$ en el conjunto no vacío A, entonces existe en el conjunto cociente $\frac{A}{\sim}$ una única ley de composición interna $*'$, tal que la aplicación canónica $\varphi : A \rightarrow \frac{A}{\sim}$ es un homomorfismo. Además, las propiedades de $*$ en A se transfieren a $*'$ en $\frac{A}{\sim}$.

Para demostrar este enunciado consideramos las siguientes etapas:




i) Sean $K_u$ y $K_v$ dos elementos de $\frac{A}{\sim}$, es decir, dos clases de equivalencia. Como la aplicación canónica $\varphi : A \rightarrow \frac{A}{\sim}$ es sobreyectiva existen $x \in A$, $y \in A$ tales que $\varphi(x)=K_u$ y $\varphi(y)=K_v$ (1). Con esto hemos logrado pasar del conjunto cociente al conjunto A, donde $*$ es una ley de composición interna, y por lo tanto $x * y \in A$.

Ahora bien, por definición de aplicación canónica, $\varphi(x * y) \in \frac{A}{\sim}$, es decir, $\varphi(x * y) = K_w$ (2).

De este modo, a partir de dos clases $K_u$ y $K_v$ hemos obtenido una clase resultante $K_w$. Para que esta asignación sea una ley de composición interna en $\frac{A}{\sim}$ hay que demostrar que $K_w$ depende exclusivamente de $K_u$ y $K_v$, y no de la elección de sus preimágenes en A. En efecto, sean $x'$ e $y'$ en A, tales que $\varphi(x') = K_u$ y $\varphi(y') = K_v$ (3). Entonces, por (1) y (3) se tiene

$$\varphi(x') = \varphi(x) \text{ y } \varphi(y') = \varphi(y) \Rightarrow x' \sim x \wedge y' \sim y \quad x' * y' \sim x * y$$

por la hipótesis de la compatibilidad; y por la definición de aplicación canónica resulta $\varphi(x' * y') = \varphi(x * y) = K_w$, con lo que nuestro propósito queda satisfecho.

Definimos ahora

$$*' : \frac{A}{\sim} \times \frac{A}{\sim} \to \frac{A}{\sim} \text{ mediante}$$

$$K_u *' K_v = \varphi(x) *' \varphi(y) = \varphi(x * y) = K_w$$

Esta definición es la traducción de lo anterior, y además queda establecido el hecho de que la aplicación canónica es un homomorfismo de A en $\frac{A}{\sim}$ respecto de $*$ y $*'$.

ii) Veamos ahora que esta ley de composición interna $*'$ es única, con la condición de que la aplicación canónica sea un homomorfismo. Para ello, supongamos que además existe $*''$ en $\frac{A}{\sim}$, con dicha condición. Entonces

$$K_u *'' K_v = \varphi(x) *'' \varphi(y) = \varphi(x * y) = \varphi(x) *' \varphi(y) = K_u *' K_v$$

Es decir: $*'' = *'$ por definición de igualdad de funciones.

iii) Además de la existencia y unicidad de la ley $*'$, inducida en A por la relación de equivalencia compatible con $*$, veamos que las propiedades de $*$ en A se verifican para $*'$ en $\frac{A}{\sim}$.

a) Asociatividad. Supongamos que $*$ sea asociativa en A. Entonces

$$(K_u *' K_v) *' K_w = [\varphi(x) *' \varphi(y)] *' \varphi(z) = \varphi(x * y) *' \varphi(z) =$$
$$= \varphi[(x * y) * z] = \varphi[x * (y * z)] = \varphi(x) *' \varphi(y * z) =$$
$$= \varphi(x) *' [\varphi(y) *' \varphi(z)] = K_u *' (K_v *' K_w)$$

b) Conmutatividad. Si $*$ es conmutativa, $*'$ también lo es. En efecto

$$K_u *' K_v = \varphi(x) *' \varphi(y) = \varphi(x * y) = \varphi(y * x) = \varphi(y) *' \varphi(x) =$$
$$= K_v *' K_u$$

c) Existencia de neutro. Si $e \in A$ es neutro, entonces $\varphi(e) = K_e$ es neutro en $\frac{A}{\sim}$.

$$\text{Sea } K_u *' K_e = \varphi(x) *' \varphi(e) = \varphi(x * e) = \varphi(x) = K_u$$

Y análogamente se verifica $K_e *' K_u = K_u$.

d) Existencia de inversos. Supongamos que $x'$ sea inverso de $x$ respecto de $*$. Entonces las correspondientes clases $K_{u'}$ y $K_u$ son inversas respecto de $*'$, pues $K_u *' K_{u'} = \varphi(x) *' \varphi(x') = \varphi(x * x') = \varphi(e) = K_e$

Análogamente se tiene $K_{u'} *' K_u = K_e$.

***Ejemplo 5-15.***

Consideremos en **Z** la adición y la multiplicación. Sabemos que la congruencia módulo $n$ es compatible con estas leyes internas, de acuerdo con los ejemplos 5-12 y 5-13. Fijemos en particular $n = 3$; el conjunto cociente es ahora el de las clases de restos módulo 3, es decir, $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

De acuerdo con el teorema fundamental de compatibilidad, existen en $Z_3$ sendas leyes de composición interna, únicas, tales que la aplicación canónica $\varphi : Z \to Z_3$ es un homomorfismo. Las leyes inducidas se llaman, respectivamente, suma y producto de clases, que simbolizamos con $\oplus$ y $\odot$. Las tablas de estas leyes internas en el conjunto de las clases son

| $\oplus$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

| $\odot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{1}$ |

La construcción de éstas se basa en el teorema fundamental; por ejemplo

$$\bar{1} \oplus \bar{2} = \varphi(1) \oplus \varphi(2) = \varphi(1 + 2) = \varphi(3) = \varphi(0) = \bar{0}$$

$$\bar{2} \odot \bar{2} = \varphi(2) \odot \varphi(2) = \varphi(2 \,.\, 2) = \varphi(4) = \varphi(1) = \bar{1}$$

En la práctica, dadas dos clases, se suman sus preimágenes en **Z** (o bien se multiplican, según sea el caso); la suma obtenida se divide por 3, y se propone como resultado en $Z_3$ la clase correspondiente al resto de la división. El esquema que proporciona la validez de este mecanismo consiste en la aplicación del teorema anterior.

***Ejemplo 5-16.***

Con análogo criterio construimos las tablas de adición y multiplicación de las clases de restos módulo 4, y obtenemos

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

| | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

Nos decidimos por denotar con los símbolos + y . la suma y el producto de clases, y nos interesa caracterizar las propiedades de estas operaciones en $\mathbf{Z}_3$ y en $\mathbf{Z}_4$. De acuerdo con el teorema fundamental, toda propiedad de la suma en **Z** se trasfiere a la suma en $\mathbf{Z}_3$ y $\mathbf{Z}_4$ y lo mismo ocurre con el producto. Sabiendo entonces que la adición es conmutativa y asociativa en **Z**, también lo es la suma de clases, y nada hay que demostrar. Además, como 0 es neutro para la adición en **Z**, resulta $\bar{0}$ neutro para la suma en $\mathbf{Z}_3$ y $\mathbf{Z}_4$. Por otra parte, como todo entero tiene inverso aditivo, la misma situación se presenta con toda clase de $\mathbf{Z}_3$ y de $\mathbf{Z}_4$. La multiplicación en **Z** es conmutativa, asociativa y con neutro igual a 1; en consecuencia, lo mismo ocurre para la multiplicación en $\mathbf{Z}_3$ y $\mathbf{Z}_4$, siendo el neutro $\bar{1}$. Avanzando un poco más en la interpretación del teorema fundamental, se dice que toda propiedad de $*$ en A, se trasfiere a $*'$ en A; pero el teorema no establece que si una propiedad no se cumple en A entonces no se cumple en $\frac{A}{\sim}$. Veamos esto a la luz de los dos ejemplos 5-15 y 5-16.

Se sabe que, en **Z**, elementos no nulos dan producto no nulo, o lo que es lo mismo: si el producto de dos factores es cero, entonces alguno de los dos es cero. Esto se traduce diciendo que en **Z** no existen divisores de cero. Pero, por lo anterior, si en **Z** no existen divisores de cero no se deduce que no existan en el cociente. En efecto, basta analizar la tabla de la multiplicación de clases para ver la existencia de divisores de cero en $\mathbf{Z}_4$, ya que $\bar{2}\,.\,\bar{2} = \bar{0}$. Es decir, existen elementos no nulos que dan producto nulo. En cambio es fácil constatar que en $\mathbf{Z}_3$ no existen divisores de cero. Más adelante demostraremos que para la no existencia de divisores de cero es condición necesaria y suficiente que el módulo de la congruencia sea primo.

## 5.6. LEY DE COMPOSICION EXTERNA

Se presenta a menudo la necesidad de operar con elementos de dos conjuntos, de modo que la composición sea un elemento de uno de ellos. Esta situación es una de las características de la estructura de espacio vectorial.

Sean dos conjuntos A y $\Omega$, este último llamado de operadores.

***Definición***

Una ley de composición externa definida en A, con operadores de $\Omega$, es toda función de $\Omega \times A$ en A.

Usualmente, una ley de composición externa en A con operadores en $\Omega$ se denota mediante ".", y suele llamarse producto de operadores de $\Omega$ por elementos de A.

En símbolos se tiene

$$\text{"."} \text{ es ley externa en A con operadores en } \Omega \Leftrightarrow . : \Omega \times A \rightarrow A$$

Mediante esta función, la imagen del par $(\alpha ; a)$ se escribe $\alpha . a$.

*Ejemplo 5-17.*

Si A es el conjunto de los segmentos contenidos en un plano y **N** es el conjunto de los números naturales, una ley de composición externa en A con operadores o escalares en **N** es el producto de números naturales por segmentos del plano.

*Ejemplo 5-18.*

Sean $\mathbf{R}^2$ y **Q**. Definimos producto de números racionales por pares ordenados de números reales, mediante

$$\alpha . (a , b) = (\alpha . a , \alpha . b)$$

La igualdad anterior determina una ley de composición externa en $\mathbf{R}^2$ con operadores en **Q**. Notamos aquí que el mismo signo "." aparece en la definición anterior con dos significados distintos: en el primer miembro se trata del producto de racionales por pares ordenados de reales, y en el segundo miembro consiste en el producto de racionales por reales.

En particular, si el conjunto A se identifica con $\Omega$, la ley externa se vuelve interna.

*Ejemplo 5-19.*

Consideremos ahora $\mathbf{R}^{n \times m}$ y **R**. Vamos a definir una ley de composición externa en $\mathbf{R}^{n \times m}$ con escalares u operadores reales, mediante

$$\alpha . A = \alpha . [a_{ij}] = [\alpha . a_{ij}] \text{ cualesquiera que sean } \alpha \in \mathbf{R} \text{ y } A \in \mathbf{R}^{n \times m}$$

Se tiene así el producto de números reales por matrices $n \times m$, y se realiza multiplicando cada elemento de la matriz por el número real.

*Ejemplo 5-20.*

Si **R** [X] denota el conjunto de todos los polinomios con coeficientes reales, y el conjunto de operadores es **R**, entonces el producto usual de números reales por polinomios es una ley de composición externa en **R** [X] con escalares en **R**.

Pero si el conjunto de operadores es el de los números complejos, el producto usual de complejos por polinomios de **R** [X] no es una ley de composición externa, pues dicho producto no es siempre un polinomio real.

## TRABAJO PRACTICO V

*5-21.* En $\mathbf{Z}$ se define $*$ por medio de $a * b = 2(a+b)$. Estudiar las propiedades y la existencia de elementos distinguidos.

*5-22.* Demostrar que si existe elemento neutro respecto de una ley de composición interna, entonces es único.

*5-23.* Formar la tabla de la composición de aplicaciones biyectivas de $A = \{1, 2, 3\}$ en sí mismo.

*5-24.* Demostrar que el inverso del inverso de un elemento, si existe, se identifica con dicho elemento.

*5-25.* Demostrar que si $a$ y $b$ admiten inversos respecto de una ley asociativa, entonces se verifica

$$(a * b)' = b' * a'$$

*5-26.* Estudiar las propiedades de $* : \mathbf{Z}^2 \to \mathbf{Z}$ tal que $a * b = a + b + 4$.

*5-27.* Determinar si la congruencia módulo 2 es compatible con $*$, en el caso del ejercicio anterior.

*5-28.* Analizar las propiedades y elementos distinguidos de $* : \mathbf{R}^2 \to \mathbf{R}$ definida por $a * b = 0$.

*5-29.* Realizar el mismo análisis con relación a $\perp : \mathbf{Q}^* \times \mathbf{Q}^* \to \mathbf{Q}^*$, tal que $x \perp y = x + \dfrac{1}{y}$ siendo $\mathbf{Q}^* = \mathbf{Q} - \{0\}$

*5-30.* En $\mathbf{R}$ se considera la ley de composición interna $*$ que asigna a cada par ordenado de reales el mínimo de los dos. Estudiar sus propiedades.

*5-31.* El conjunto $\mathbf{R}^{\mathbf{I}}$, donde I es el intervalo cerrado $[0, 1]$, consiste en todas las funciones de I en $\mathbf{R}$, es decir

$$\mathbf{R}^{\mathbf{I}} = \{ f \,/\, f : \mathbf{I} \to \mathbf{R} \}$$

En $\mathbf{R}^{\mathbf{I}}$ se define la suma de funciones mediante $(f+g)(x) = f(x) + g(x)$ para todo $x \in \mathbf{I}$. Estudiar las propiedades de esta ley interna.

*5-32.* Confeccionar la tabla de la composición de funciones del conjunto $S^S$, donde $S = \{a, b\}$.

*5-33.* La función $f: \mathbf{R}^2 \to \mathbf{R}$ es una ley interna en $\mathbf{R}$ definida por $f(a, b) = a + b^2$. Verificar que no es asociativa ni conmutativa, ni admite neutro.

*5-34.* Se sabe que $*$ es una ley de composición interna en A, que satisface

$$\forall a, \forall b, \forall c, \forall d: (a * b) * (c * d) = (a * c) * (b * d)$$

Demostrar que $*$ es asociativa y conmutativa, si existe neutro.

*5-35.* En $\mathbf{Q}^*$ se define $*$ tal que $a * b = 3\,a\,b$. Verificar que $*$ es asociativa, con neutro, conmutativa, y además todos los elementos son inversibles.

*5-36.* En $\mathbf{\mathring{R}}^{\mathbf{I}}$ se define el producto de funciones por medio de $(f\,.\,g)(x) = f(x)\,.\,g(x)$ cualquiera que sea $x \in \mathrm{I}$. Demostrar la asociatividad, conmutatividad, existencia de neutro, y la distributividad respecto de la suma de funciones definida en el ejercicio 5-31.

*5-37.* $*$ es una ley de composición externa en $\mathbf{C}$ con escalares reales, es decir: $*: \mathbf{R} \times \mathbf{C} \to \mathbf{C}$ tal que $a * z = a\,.\,z$. Verificar las siguientes propiedades:

i ) $a * (b * z) = (a\,.\,b) * z$

ii ) $(a + b) * z = (a * z) + (b * z)$

iii) $a * (z + w) = (a * z) + (a * w)$

*5-38.* Se consideran $\mathbf{R}^+$ con el producto y $\mathbf{R}$ con la suma. Probar que la función $f: \mathbf{R}^+ \to \mathbf{R}$, tal que $f(x) = \log_2 x$, es un morfismo biyectivo.

*5-39.* Demostrar que la aplicación $f: \mathbf{Z} \to \{-1, 0, 1\}$ es un morfismo respecto del producto en ambos conjuntos, siendo $f(x) = sg\,(x)$.

*5-40.* En $\mathbf{N}$ se definen las leyes de composición interna $*$ y $\circ$ mediante

$$x * y = x$$

$$x \circ y = x + y$$

Investigar las distributividades de $*$ respecto de $\circ$.

Capítulo 6

# COORDINABILIDAD. INDUCCION COMPLETA. COMBINATORIA

## 6.1. INTRODUCCION

En esta sección se propone al lector el estudio de la relación de coordinabilidad o equipotencia entre conjuntos, sobre la base de un tratamiento funcional, y se introduce como derivación natural el concepto de número cardinal de un conjunto. Por esta vía se define el número natural, pero el estudio de las operaciones y propiedades se desarrollará sobre la base del sistema axiomático de Peano, en el capítulo siguiente. En conexión con **N**, se da el principio de inducción completa con vistas a la demostración de propiedades en las que todo estudiante de un curso básico debe ejercitarse. Asimismo, se trata un tema de vastas aplicaciones en matemática elemental y en Probabilidades; tal es el caso de la combinatoria simple y con repetición, lo que se reduce, en última instancia, a la no fácil tarea de saber contar los elementos de un conjunto.

## 6.2. CONJUNTOS COORDINABLES O EQUIPOTENTES

### 6.2.1. Concepto

Sea U un conjunto. En $P$ (U) definimos la siguiente relación: "dos elementos de $P$(U), es decir, dos subconjuntos de U, son coordinables si y sólo si existe una biyección del primero en el segundo".

Simbólicamente

$$A \sim B \Leftrightarrow \exists f : A \rightarrow B \,/\, f \text{ es biyectiva} \qquad (1)$$

Esta relación satisface

i ) *Reflexividad.* Todo conjunto es coordinable a sí mismo.

Sea $A \in P$ (U). Como existe

$i_A : A \rightarrow A$ , y es biyectiva, por (1) resulta $A \sim A$.

ii) *Simetría.* Si un conjunto es coordinable a otro, entonces éste es coordinable al primero.

Sea A ~B. Entonces $\exists f : A \to B \mid f$ es biyectiva.

Por 4.7.2. II), sabemos que $f$ admite inversa, es decir

$$\exists f^{-1} : B \to A \mid f^{-1} \text{ es biyectiva,}$$

lo que significa, por (1), que B~A.

iii) *Transitividad.* Si un conjunto es coordinable a otro, y éste es coordinable con un tercero, entonces el primero es coordinable con el tercero.

Se trata de probar

$$A \sim B \text{ y } B \sim C \Rightarrow A \sim C$$

Demostración)

$$A \sim B \ \wedge \ B \sim C \qquad \text{Por hipótesis}$$

$$\Downarrow$$

$$\exists f : A \to B \ \wedge \ g : B \to C \mid f \text{ y } g \text{ son biyectivas.} \qquad \text{Por (1)}$$

$$\Downarrow$$

$$\exists g \circ f : A \to C \mid g \circ f \text{ es biyectiva.}$$ Porque la composición de funciones biyectivas es biyectiva, según 4.6.5.

$$\Downarrow$$

$$A \sim C \qquad \text{Por (1)}$$

Ahora bien, de acuerdo con el teorema fundamental de las relaciones de equivalencia, existe una partición de $P$ (U) en clases de equivalencia, las cuales reciben el nombre de números cardinales de los subconjuntos de U.

***Definición***

Número cardinal del subconjunto A ⊂ U, es la totalidad de los subconjuntos de U que son coordinables a A.

En símbolos

$$c(A) = \{ X \in P(U) \mid X \sim A \}$$

Se tiene

$$c(A) = c(B) \Leftrightarrow A \sim B$$

En particular $c(\phi) = 0$, es decir, denotamos con 0 el número cardinal del conjunto vacío.

Si $a \in U$, entonces $c(\{a\}) = 1$.

Si $a$ y $b \in U$, entonces $c(\{a, b\}) = 2$.

Es decir, los números cardinales de las partes finitas y no vacías de U son números naturales.

Con $N_0$ denotamos el conjunto $N \cup \{0\}$.

***Ejemplo 6-1.***

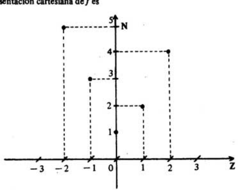
Se trata de probar que N y Z son conjuntos coordinables.

De acuerdo con la definición, es suficiente proponer una función biyectiva de N en Z, o lo que es lo mismo, de Z en N, por la simetría de la relación. Para ello definimos

$$f: Z \to N \text{ mediante}$$

$$f(x) = \begin{cases} 2x & \text{si } x > 0 \\ -2x + 1 & \text{si } x \leq 0 \end{cases}$$

La representación cartesiana de $f$ es




y el lector puede comprobar que $f$ es biyectiva. En consecuencia, Z y N son coordinables o equipotentes.

## 6.3. CONJUNTOS FINITOS Y NUMERABLES

### 6.3.1. Conjunto finito

**i ) *Definición***

Intervalo natural inicial $I_n$ es el conjunto de los $n$ primeros números naturales.

$$I_n = \{1, 2, \ldots n\}$$

ii ) *Definición*

Un conjunto es finito si y sólo si es vacío, o coordinable a un intervalo natural inicial

$$A \text{ es finito} \Leftrightarrow A = \phi \ \vee \ \exists\, n \in N \,/\, A \sim I_n.$$

iii) *Definición*

Un conjunto es infinito si y sólo si no es finito.

Los números cardinales asociados a los conjuntos finitos son el 0 o los números naturales. Los números cardinales correspondientes a los conjuntos infinitos se llaman trasfinitos. El número cardinal de un conjunto especifica la "numerosidad" de los elementos del conjunto, o lo que es lo mismo, su potencia. En el caso de los conjuntos infinitos existe una jerarquización relativa a sus números cardinales, como veremos más adelante.

### 6.3.2. Conjunto numerable y sucesión

i ) *Definición*

Un conjunto es numerable si y sólo si es coordinable a N.

$$A \text{ es numerable} \Leftrightarrow A \sim N \Leftrightarrow \exists\, f: A \to N \,/\, f \text{ es biyectiva.}$$

Un conjunto infinito no coordinable a N se llama no numerable. Para indicar que un conjunto puede ser finito o coordinable a N, suele decirse que es "a lo sumo numerable".

ii ) *Propiedad.* Un conjunto es numerable si y sólo si sus elementos constituyen la imagen de una sucesión.

Si A es numerable es coordinable a N, y esto significa que existe una función biyectiva de N en A, es decir, una sucesión de elementos de A cuyo conjunto imagen es exactamente A.

La representación de A es entonces

$$A = \left\{ a_1, a_2, \ldots, a_n, \ldots \right\} \qquad (1)$$

Recíprocamente, si A es del tipo (1), entonces es coordinable a $\dot{N}$ mediante la asignación $f(n) = a_n$, y en consecuencia es numerable.

*Ejemplo 6-2.*

i ) El conjunto $A = \left\{ \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots \right\}$ es numerable, por ser la imagen de la sucesión

$$f: N \to A \quad \text{definida por} \quad f(n) = \frac{n}{n+1}$$

ii ) La unión de dos conjuntos disjuntos, uno finito y el otro numerable, es numerable.

Sean A finito, y B numerable, tales que $A \cap B = \phi$.

a) Si A es vacío, $A \cup B = B$, y por lo tanto la unión es numerable.

b) Consideremos el caso en que A es finito y no vacío. Entonces es coordinable a un intervalo natural inicial $I_n$, y puede denotarse

$$A = \{a_1, a_2, \ldots, a_n\}$$
$$B = \{b_1, b_2, \ldots, b_n, \ldots\}$$

Se tiene

$$A \cup B = \{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots\}$$

Definimos

$$f: A \cup B \to \mathbf{N} \text{ por medio de}$$

$$f(x) = \begin{cases} i & \text{si } x = a_i \\ n + i & \text{si } x = b_i \end{cases}$$

Es fácil ver que $f$ es biyectiva y, en consecuencia, $A \cup B \sim \mathbf{N}$, con lo que la propiedad queda demostrada.

El mismo **N** es numerable, teniendo en cuenta la reflexividad de la relación de coordinabilidad. De acuerdo con el ejemplo 6-1, también **Z** es numerable, es decir, ambos tienen el mismo número cardinal trasfinito, o sea, tienen "el mismo número de elementos". El número cardinal de **N**, introducido por George Cantor, es $\aleph$ aleph cero, lo denotaremos con $a$, y escribimos

$$c(\mathbf{N}) = c(\mathbf{Z}) = a$$

En el ejemplo 4-10 se demostró la biyectividad entre **N** y P, siendo P el conjunto de los números pares positivos, es decir: $P \sim \mathbf{N}$, y por consiguiente tienen el mismo número cardinal. Puede escribirse $c(P) = a$, y se dice que el conjunto de los números naturales pares es equipotente a **N**, a pesar de ser una parte propia de **N**.

Esta propiedad es característica de todo conjunto infinito, en el sentido siguiente: "un conjunto es infinito si y sólo si es coordinable a una parte propia del mismo".

$$A \text{ es infinito} \Leftrightarrow \exists\, X \subsetneq A \,/\, X \sim A$$

## 6.4. INDUCCION COMPLETA

### 6.4.1. Concepto:

El principio de inducción completa proporciona un método de demostración por recurrencia, de vastas aplicaciones en matemática. No es constructivo, en el sentido de generar propiedades; pero hace posible la demostración de éstas cuando son relativas al conjunto de los números naturales.

A fin de tener una idea intuitiva de dicho principio, consideremos el siguiente caso: supongamos alineado el conjunto de todos los alumnos de una escuela; se sabe además que, si un alumno habla, entonces habla el siguiente. Interesa determinar cuál es la condición para asegurar que, en un momento dado, estén hablando todos los alumnos. Es obvio que para que se dé esa situación es suficiente ver que el primero está hablando. En este caso se trata de investigar la propiedad que podemos enunciar así: "todos los alumnos están hablando", y para asegurar su verdad se requieren las siguientes condiciones:

i ) El primer alumno habla.

ii ) Si un alumno habla, entonces habla el siguiente.

Extendiendo el caso a una propiedad P, relativa al conjunto de los números naturales, queda asegurada la verdad de P para todo $n \in \mathbf{N}$, si se verifican las dos condiciones anteriores, que se traducen en

i ) $P(1)$ es V.

ii ) Si $P(h)$ es V, entonces $P(h+1)$ es V.

Llegaremos a la demostración de este principio, llamado de inducción completa, sobre la base del principio de buena ordenación, que según 3.9.7. admite el siguiente enunciado: "todo subconjunto no vacío de N tiene primer elemento"

### 6.4.2. Teorema de inducción completa

Si S es un subconjunto de N que satisface

i ) $1 \in S$

ii ) $h \in S \Rightarrow h+1 \in \mathbf{N}$

entonces $S = \mathbf{N}$.

En otras palabras: "todo subconjunto de N que incluya al 1, y al siguiente de $h$ siempre que incluya al $h$, es igual a N".

Hipótesis) $S \subset \mathbf{N}$

i ) $1 \in S$

ii ) $h \in S \Rightarrow h+1 \in S$

Tesis) $S = \mathbf{N}$.

Demostración) Es suficiente ver que $\mathbf{N} \subset S$, y para esto basta probar que el subconjunto S' de números naturales no pertenecientes a S es vacío; o sea, de acuerdo con la definición de inclusión es falso que haya algún natural que no pertenezca a S.

Suponemos que $S' \neq \phi$. Por tratarse de un subconjunto no vacío de N, de acuerdo con el principio de buena ordenación, existe el elemento mínimo $m \in S'$ (1).

Por hipótesis, $1 \in S$, y como los elementos de S' no pertenecen a S, es $m \neq 1$. Por otra parte, siendo $m$ natural y distinto de 1, se tiene

$$m > 1$$

y, en consecuencia $$m - 1 > 0.$$

Como $m - 1 < m$, por ser $m$ el mínimo de S', resulta $m - 1 \in S$.

Ahora bien, de acuerdo con la hipótesis ii )

$$m - 1 \in S \Rightarrow (m-1) + 1 \in S \Rightarrow m \in S$$

Esta proposición es contradictoria con (1). Luego $N \subset S$, y como por hipótesis $S \subset N$, resulta $S = N$.

### 6.4.3. Principio de inducción completa

Sea P ($n$) una función proposicional, donde $n \in N$. Si ocurre que P (1) es verdadera, y, además, de la verdad de P ($h$) se deduce la verdad de P ($h$ + 1), entonces P ($n$) es verdadera para todo $n$.

Hipótesis) P (1) es V

$$\forall h : P(h) \Rightarrow P(h+1)$$

Tesis) $\forall n : P(n)$ es V.

Demostración)

> El subconjunto S de números naturales para los cuales P ($n$) es verdadera, contiene al 1, y al siguiente de $h$ siempre que contenga a $h$. Luego, por el teorema 6.4.2., S = N. Es decir, P ($n$) es V para todo $n \in N$.

*Nota:*

La demostración de una propiedad relativa a N por inducción completa, se realiza probando la verdad de las dos proposiciones de la hipótesis del teorema anterior.

***Ejemplo 6-3.***

Demostramos por inducción completa:

a) La suma de los $n$ primeros números naturales es $\dfrac{n(n+1)}{2}$.

Es decir, $\forall n \in N$ se verifica

$$S_n = 1 + 2 + \ldots + n = \frac{n\ (n+1)}{2}$$

i ) Debemos probar que la propiedad se verifica para $n = 1$. En este caso, la suma se reduce al primer término, y se tiene

$$S_1 = 1 = \frac{1 \,.\, (1+1)}{2}$$

ii ) Demostramos la verdad de la implicación de la hipótesis del principio de inducción completa, es decir, el siguiente teorema

Hipótesis) $$S_h = 1 + 2 + \ldots + h = \frac{h\ (h+1)}{2}$$

Tesis) $$S_{h+1} = 1 + 2 + \ldots + h + (h+1) = \frac{(h+1)\ (h+2)}{2}$$

Demostración) Teniendo en cuenta la hipótesis inductiva, el primer miembro de la tesis se trasforma en

$$S_{h+1} = 1 + 2 + \ldots + h + (h+1) = S_h + (h+1) = \frac{h\ (h+1)}{2} + (h+1)$$

Reduciendo a común denominador, y por distributividad

$$S_{h+1} = \frac{h\ (h+1) + 2\ (h+1)}{2} = \frac{(h+1)\ (h+2)}{2}$$

Resulta entonces la fórmula anterior, válida para todo número natural $n$. De acuerdo con ella, la suma de los 10 primeros números naturales es $S_{10} = \frac{10 \,.\, 11}{2} = 55$.

b) Probaremos ahora

$$S_n = \frac{1}{1 \,.\, 2} + \frac{1}{2 \,.\, 3} + \frac{1}{3 \,.\, 4} + \cdots + \frac{1}{n\,(n+1)} = \frac{n}{n+1}$$

i ) $n = 1 \Rightarrow S_1 = \frac{1}{1 \,.\, 2} = \frac{1}{2} = \frac{1}{1+1}$

ii ) $P(h)$ es V $\Rightarrow P(h+1)$ es V

Hipótesis) $S_h = \frac{h}{h+1}$

Tesis) $S_{h+1} = \frac{h+1}{h+2}$

Demostración) Procediendo como en el caso anterior

$$S_{h+1} = \frac{1}{1 \,.\, 2} + \frac{1}{2 \,.\, 3} + \cdots + \frac{1}{h\,(h+1)} + \frac{1}{(h+1)\,(h+2)} =$$

$$= S_h + \frac{1}{(h+1)\,(h+2)} = \frac{h}{h+1} + \frac{1}{(h+1)\,(h+2)} =$$

$$= \frac{h\,(h+2) + 1}{(h+1)\,(h+2)} = \frac{h^2 + 2\,h + 1}{(h+1)\,(h+2)} =$$

$$= \frac{(h+1)^{\not 2}}{\cancel{(h+1)}\,(h+2)} = \frac{h+1}{h+2}$$

## 6.5. EL SIMBOLO DE SUMATORIA

### 6.5.1. Concepto.

En muchas situaciones se presenta la conveniencia de abreviar la notación de una suma cuyos términos admiten cierta ley de formación. En este sentido es útil la introducción del símbolo de sumatoria: $\Sigma$.

Si $a_i$ es un número real que depende del índice $i$, para indicar la suma $a_1 + a_2 + a_3 + a_4 + a_5$ escribimos $\sum\limits_{i=1}^{5} a_i$.

Si el índice es variable desde 1 a $n$, la notación $\sum\limits_{i=1}^{n} a_i$ significa la suma abreviada de los $n$ términos $a_1 + a_2 + \cdots + a_n$, y se lee: "sumatoria de $a_i$ con $i$ variando desde 1 a $n$".

El desarrollo de una sumatoria se obtiene asignando a $i$, cada uno de los sucesivos valores de su rango de variación, y sumando los términos así obtenidos. Por ejemplo

$$\sum_{i=1}^{4} i^2 = 1^2 + 2^2 + 3^2 + 4^2$$

*Ejemplo 6-4.*

Desarrollar las siguientes sumatorias:

a) $$\sum_{i=1}^{4} \frac{(-1)^i}{i} = \frac{(-1)^1}{1} + \frac{(-1)^2}{2} + \frac{(-1)^3}{3} + \frac{(-1)^4}{4} =$$
$$= -1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4}$$

b) $$\sum_{i=1}^{n} \frac{2\,i}{i+1} = \frac{2\,.\,1}{1+1} + \frac{2\,.\,2}{2+1} + \frac{2\,.\,3}{3+1} + \cdots + \frac{2\,n}{n+1} =$$
$$= 1 + \frac{4}{3} + \frac{6}{4} + \cdots + \frac{2\,n}{n+1}$$

c) $$\sum_{i=1}^{3} (i-1) = (1-1) + (2-1) + (3-1) =$$
$$= 0 + 1 + 2 = 3$$

d) $$\sum_{i=1}^{n} a = \underbrace{a + a + \ldots + a}_{n} = n\,a$$

Aquí se tiene $a_i = a \ \forall i$.

e) $\sum_{i=1}^{100} 1 = \underbrace{1 + 1 + \ldots + 1}_{100} = 100$

f) $\sum_{k=0}^{3} \frac{-k+1}{k+2} = \frac{1}{2} + 0 - \frac{1}{4} - \frac{2}{5}$

***Ejemplo 6-5.***

Expresar como sumatorias las siguientes sumas indicadas:

a) $2 + 4 + 6 + 8 + 10 = \sum_{i=1}^{5} 2i$

b) $1 + 3 + 5 + 7 + 9 + 11 = \sum_{i=1}^{6} (2i - 1) = \sum_{i=0}^{5} (2i + 1)$

c) $1 + 8 + 27 + 64 = \sum_{i=1}^{4} i^3$

d) $2 + \frac{3}{2} + \frac{4}{3} + \frac{5}{4} + \frac{6}{5} = \sum_{i=1}^{5} \frac{i+1}{i}$

**6.5.2. Propiedades de la sumatoria**

i ) $\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$

En efecto, por definición de sumatoria, conmutatividad y asociatividad de la suma en **R**, se tiene

$$\sum_{i=1}^{n} (a_i + b_i) = (a_1 + b_1) + (a_2 + b_2) + \ldots + (a_n + b_n) =$$
$$= (a_1 + a_2 + \ldots + a_n) + (b_1 + b_2 + \ldots + b_n) =$$
$$= \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$$

ii ) $\sum_{i=1}^{n} (a\, a_i) = a \sum_{i=1}^{n} a_i$ donde $a$ es constante.

Por definición de sumatoria y distributividad resulta

$$\sum_{i=1}^{n} (a\, a_i) = a\ a_1 + a\ a_2 + \ldots + a\, a_n =$$
$$= a\,(a_1 + a_2 + \ldots + a_n) = a \sum_{i=1}^{n} a_i$$

***Ejemplo 6-6.***

Reducir

$$\sum_{i=1}^{n} (x_i + 1)^2 = \sum_{i=1}^{n} (x_i^2 + 2x_i + 1) = \sum_{i=1}^{n} x_i^2 + \sum_{i=1}^{n} 2x_i + \sum_{i=1}^{n} 1 =$$

$$= \sum_{i=1}^{n} x_i^2 + 2\sum_{i=1}^{n} x_i + n$$

***Ejemplo 6-7.***

Dados $n$ números reales $x_1, x_2, \ldots, x_n$, se define el promedio $\overline{X}$ ($x$ raya) mediante

$$\overline{X} = \frac{x_1 + x_2 + \ldots + x_n}{n} = \frac{\sum_{i=1}^{n} x_i}{n} \qquad (1)$$

Comprobar que

$$\sum_{i=1}^{n} (x_i - \overline{X})^2 = \sum_{i=1}^{n} x_i^2 - n\overline{X}^2$$

Se tiene

$$\sum_{i=1}^{n} (x_i - \overline{X})^2 = \sum_{i=1}^{n} (x_i^2 - 2\overline{X}x_i + \overline{X}^2) =$$

$$= \sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n} 2\overline{X}x_i + \sum_{i=1}^{n} \overline{X}^2 =$$

$$= \sum_{i=1}^{n} x_i^2 - 2\overline{X}\sum_{i=1}^{n} x_i + n\overline{X}^2 \qquad (2)$$

Hemos aplicado el desarrollo de un binomio, las propiedades i ) y ii ), y el ejemplo 6-4 d).

Ahora bien, por (1)

$$\sum_{i=1}^{n} x_i = n\overline{X}$$

que sustituido en (2) conduce a

$$\sum_{i=1}^{n} (x_i - \overline{X})^2 = \sum_{i=1}^{n} x_i^2 - 2\overline{X}n\overline{X} + n\overline{X}^2 =$$

$$= \sum_{i=1}^{n} x_i^2 - n\overline{X}^2$$

Esta fórmula es de aplicación frecuente en Estadística.

*Nota:*

En términos de sumatorias, las fórmulas demostradas en el ejemplo 6-3 se traducen en

a) $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

b) $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$

***Ejemplo 6-8.***

Demostrar por inducción completa

$$\sum_{i=1}^{n} i^3 = \frac{n^2 (n+1)^2}{4}$$

i ) $n = 1 \Rightarrow \sum_{i=1}^{1} i^3 = 1^3 = 1 = \frac{1 \cdot 4}{4} = \frac{1^2 \cdot (1+1)^2}{4}$

y la fórmula es válida para $n = 1$.

ii ) Hipótesis) $\sum_{i=1}^{h} i^3 = \frac{h^2 (h+1)^2}{4}$

Tesis) $\sum_{i=1}^{h+1} i^3 = \frac{(h+1)^2 (h+2)^2}{4}$

Demostración)

$$\sum_{i=1}^{h+1} i^3 = \sum_{i=1}^{h} i^3 + (h+1)^3 = \frac{h^2 (h+1)^2}{4} + (h+1)^3 =$$

$$= \frac{h^2 (h+1)^2 + 4(h+1)^3}{4} = (h+1)^2 \frac{h^2 + 4(h+1)}{4} =$$

$$= (h+1)^2 \cdot \frac{h^2 + 4h + 4}{4} = \frac{(h+1)^2 (h+2)^2}{4}$$

***Ejemplo 6-9.***

Demostrar que la suma de los $n$ primeros números naturales impares, es $n^2$.
La expresión de un número natural impar es del tipo $(2i - 1)$ con $i \in \mathbf{N}$.
Entonces

$$S_n = \sum_{i=1}^{n} (2i - 1) = 1 + 3 + 5 + \ldots + (2n - 1)$$

siendo $(2n - 1)$ el $n$-simo número impar.

i ) $n = 1 \Rightarrow S_1 = \sum_{i=1}^{1} (2i - 1) = 1 = 1^2$

ii ) Demostramos

$$S_h = h^2 \Rightarrow S_{h+1} = (h+1)^2$$

En efecto

$S_{h+1} = S_h + (2h + 1)$, donde $(2h + 1)$ es el número impar de lugar $(h + 1)$. Aplicando la hipótesis y efectuando operaciones

$$S_{h+1} = h^2 + (2h + 1) = (h + 1)^2$$

***Ejemplo 6-10.***

Demostrar

$$S_n = \sum_{i=1}^{n} 2^i = 2^{n+1} - 2$$

i ) $n = 1 \Rightarrow S_1 = \sum_{i=1}^{1} 2^i = 2^1 = 2 = 4 - 2 = 2^{1+1} - 2$

Es decir, P (1) es V.

ii ) Se trata de probar que

$$S_h = 2^{h+1} - 2 \Rightarrow S_{h+1} = 2^{h+2} - 2$$

Demostración)

$$S_{h+1} = \sum_{i=1}^{h+1} 2^i = 2 + 2^2 + \ldots + 2^h + 2^{h+1} =$$
$$= S_h + 2^{h+1} = 2^{h+1} - 2 + 2^{h+1}$$
$$\Rightarrow S_{h+1} = 2^{h+1} + 2^{h+1} - 2$$

La reducción de los dos primeros términos conduce a

$$S_{h+1} = 2 \cdot 2^{h+1} - 2$$

y por producto de potencias de igual base resulta

$$S_{h+1} = 2^{h+2} - 2$$

como queríamos.

***Ejemplo 6-11.***

Demostrar que

$$n > \left(1 + \frac{1}{n}\right)^n \qquad \forall n \geqslant 3$$

Debemos probar que P ($n$) es V, cualquiera que sea $n$, a partir de 3. En este caso, es posible aplicar el principio de inducción, demostrando

i ) P (3) es V

ii ) P ($h$) $\Rightarrow$ P ($h + 1$)

a) Sea $n = 3$. $$3 > \frac{64}{27} = \left(\frac{4}{3}\right)^3 = \left(1 + \frac{1}{3}\right)^3$$

b) Hipótesis) $h > \left(1 + \frac{1}{h}\right)^h$

Tesis) $h + 1 > \left(1 + \frac{1}{h+1}\right)^{h+1}$

Demostración)

$$\left(1 + \frac{1}{h+1}\right)^{h+1} = \left(1 + \frac{1}{h+1}\right)^h \left(1 + \frac{1}{h+1}\right) \qquad (1)$$

Por otra parte

$$\frac{1}{h+1} < \frac{1}{h} \Rightarrow 1 + \frac{1}{h+1} < 1 + \frac{1}{h} \Rightarrow$$
$$\Rightarrow \left(1 + \frac{1}{h+1}\right)^h < \left(1 + \frac{1}{h}\right)^h \Rightarrow$$
$$\Rightarrow \left(1 + \frac{1}{h+1}\right)^h \left(1 + \frac{1}{h+1}\right) < \left(1 + \frac{1}{h}\right)^h \left(1 + \frac{1}{h+1}\right) \qquad (2)$$

De (1) y (2)

$$\left(1 + \frac{1}{h+1}\right)^{h+1} < \left(1 + \frac{1}{h}\right)^h \left(1 + \frac{1}{h+1}\right)$$

Por hipótesis

$$\left(1 + \frac{1}{h}\right)^h < h$$

Multiplicando las dos últimas desigualdades, después de cancelar, nos queda

$$\left(1 + \frac{1}{h+1}\right)^{h+1} < h \left(1 + \frac{1}{h+1}\right)$$

Por distributividad

$$\left(1 + \frac{1}{h+1}\right)^{h+1} < h + \frac{h}{h+1} \qquad (3)$$

Como $h < h + 1 \Rightarrow \frac{h}{h+1} < 1 \Rightarrow h + \frac{h}{h+1} < h + 1 \qquad (4)$

Por transitividad, de (3) y (4) resulta

$$\left(1 + \frac{1}{h+1}\right)^{h+1} < h + 1$$

## 6.6. LA FUNCION FACTORIAL

### 6.6.1. *Definición*

Función factorial es la aplicación

$$f: \mathbf{N}_0 \to \mathbf{N} \text{ definida por}$$

$$\begin{cases} f(0) = 1 \\ f(1) = 1 \\ f(h+1) = (h+1) \,.\, f(h) \quad \text{si } h > 1 \end{cases}$$

El símbolo característico de la función factorial es !, en lugar de $f$, y se escribe $h\,!$ para indicar $f(h)$. De este modo lo anterior se traduce en

$$\begin{cases} 0! = 1 \\ 1! = 1 \\ (h+1)! = (h+1) \,.\, h! \end{cases}$$

La expresión $h!$ se lee "factorial de $h$" o "$h$ factorial".

La función factorial, es no inyectiva, pues $0 \neq 1$ y $0! = 1!$

### 6.6.2. Propiedad

El factorial del número natural $n \geqslant 2$ es igual al producto de los $n$ primeros números naturales.

$$n! = 1 \,.\, 2 \,.\, 3 \,\ldots\ldots\, n = n \,.\, (n-1) \,.\, (n-2) \,\ldots\ldots\, 3 \,.\, 2 \,.\, 1$$

Lo demostramos por inducción completa

i ) Si $n = 2$, entonces por definición se tiene

$$2! = 2 \,.\, 1! = 2 \,.\, 1$$

ii ) Hipótesis) $h! = 1 \,.\, 2 \,.\, 3 \,\ldots\ldots\, (h-1) \,.\, h$

Tesis) $(h+1)! = 1 \,.\, 2 \,.\, 3 \,\ldots\ldots\, h \,.\, (h+1)$

Demostración)

Aplicando al primer miembro de la tesis la definición de factorial, y la hipótesis inductiva, se tiene

$$(h+1)! = (h+1) \,.\, h! = (h+1) \,.\, h \,.\, (h-1) \,\ldots\ldots\, 3 \,.\, 2 \,.\, 1$$

con lo que el teorema queda demostrado.

*Nota:*

Es claro que la función factorial no es sobreyectiva, pues existen naturales que no se identifican con el factorial de ninguno; tal es el caso de 7, que carece de preimagen en $N_0$.

Por otra parte, para el cálculo, es muy útil tener en cuenta, de acuerdo con la definición, que el factorial de un número es igual al producto de dicho número por el factorial del anterior.

Así, $7! = 7 . 6! = 7 . 6 . 5!$

***Ejemplo 6-12.***

Verificar la igualdad

$$\frac{n}{(n+1)!} = \frac{1}{n!} - \frac{1}{(n+1)!}$$

En efecto

$$\frac{1}{n!} - \frac{1}{(n+1)!} = \frac{n+1}{(n+1)\,n!} - \frac{1}{(n+1)!} =$$

$$= \frac{n+1}{(n+1)!} - \frac{1}{(n+1)!} = \frac{n+1-1}{(n+1)!} = \frac{n}{(n+1)!}$$

## 6.7. NUMEROS COMBINATORIOS

### 6.7.1. *Definición*

Sean los enteros no negativos $n$ y $k$, tales que $n \geqslant k$. Llamamos número combinatorio "$n$ sobre $k$", al símbolo $\binom{n}{k}$ definido por

$$\binom{n}{k} = \frac{n!}{k!\ (n-k)!}$$

Los elementos de un número combinatorio se llaman numerador y denominador.

Así, $\binom{7}{3} = \frac{7!}{3!\ 4!} = \frac{7 . 6 . 5 . 4!}{3!\ 4!} = \frac{7 . 6 . 5}{3 . 2 . 1} = 35$

Se presentan los siguientes casos especiales:

$$\binom{0}{0} = \frac{0!}{0!\ 0!} = 1 \qquad \binom{n}{1} = \frac{n!}{1!\ (n-1)!} = \frac{n\,(n-1)!}{(n-1)!} = n$$

$$\binom{n}{0} = \frac{n!}{0!\ n!} = 1 \qquad \binom{n}{n} = \frac{n!}{n!\ 0!} = 1$$

$$\binom{n+1}{n} = \frac{(n+1)!}{n!\ 1!} = \frac{(n+1)\,n!}{n!} = n+1$$

### 6.7.2. Propiedades de los números combinatorios

Si dos números combinatorios de igual numerador son tales que la suma de sus denominadores coincide con aquél, se llaman números combinatorios de órdenes complementarios. Por ejemplo $\binom{7}{3}$ y $\binom{7}{4}$.

i ) Dos números combinatorios de órdenes complementarios son iguales

$$\binom{n}{k} = \frac{n!}{k!\ (n-k)!} = \frac{n!}{(n-k)!\ k!} = \binom{n}{n-k}$$

ii ) La suma de dos números combinatorios no es, en general, un número combinatorio; pero si tienen igual numerador y denominadores consecutivos vale la fórmula

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$$

En efecto

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!\ [(n-1)-(k-1)]!} + \frac{(n-1)!}{k!\ (n-1-k)!}$$

$$= \frac{(n-1)!}{(k-1)!\ (n-k)!} + \frac{(n-1)!}{k!\ (n-k-1)!} =$$

$$= \frac{k\,(n-1)!}{k\ (k-1)!\ (n-k)!} + \frac{(n-k)\ (n-1)!}{k!\ (n-k)\ (n-k-1)!} =$$

$$= \frac{k\ (n-1)!}{k!\ (n-k)!} + \frac{(n-k)\ (n-1)!}{k!\ (n-k)!} =$$

$$= \frac{k\,(n-1)! + (n-k)\,(n-1)!}{k!\ (n-k)!} = \frac{(n-1)!\ (\not{k} + n - \not{k})}{k!\ (n-k)!} =$$

$$= \frac{n\,(n-1)!}{k!\ (n-k)!} = \frac{n!}{k!\ (n-k)!} = \binom{n}{k}$$

*Ejemplo 6-13.*

i ) Formamos el "triángulo" de Pascal

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

- - - - - - - - - - - - - - - - - - - - - - -

Los elementos extremos de cada fila valen 1, y cada número combinatorio restante de acuerdo con la propiedad ii ), es la suma de los dos que figuran sobre él.

ii ) Probar

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-2}{n-1} + \ldots \binom{n}{n-1} + \binom{n-1}{n-1}$$

Es decir

$$\binom{m}{n} = \sum_{i=1}^{m-n+1} \binom{m-i}{n-1}$$

Aplicando reiteradamente la propiedad ii ) se tiene

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n} = \binom{m-1}{n-1} + \binom{m-2}{n-1} + \binom{m-2}{n} =$$

$$= \binom{m-1}{n-1} + \binom{m-2}{n-1} + \binom{m-3}{n-1} + \binom{m-3}{n} =$$

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

$$= \binom{m-1}{n-1} + \binom{m-2}{n-1} + \binom{m-3}{n-1} + \cdots + \binom{n}{n-1} + \binom{n}{n} =$$

$$= \binom{m-1}{n-1} + \binom{m-2}{n-1} + \binom{m-3}{n-1} + \cdots + \binom{n}{n-1} + \binom{n-1}{n-1}$$

iii) Demostrar

$$\binom{n}{k} = \frac{n(n-1)(n-2)\ldots(n-k+1)}{k!}$$

Aplicando la definición y la nota que figura en 6.6.1, tenemos

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n(n-1)(n-2)\ldots(n-k+1)(n-k)!}{k!\,(n-k)!}$$

Después de simplificar queda

$$\binom{n}{k} = \frac{n(n-1)(n-2)\ldots(n-k+1)}{k!}$$

## 6.8. POTENCIA DE UN BINOMIO

### 6.8.1. Binomio de Newton

Una aplicación inmediata de los números combinatorios se presenta en el desarrollo de la potencia de un binómio, con exponente natural, conocido como fórmula del binomio de Newton, y está dada por

$$(a+b)^n = \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1} b^1 + \binom{n}{2}a^{n-2} b^2 + \ldots + \binom{n}{n}a^0 b^n$$

Utilizando el símbolo de sumatoria, se reduce a

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

y la demostramos por inducción completa.

i ) $n = 1 \Rightarrow (a+b)^1 = a + b = a^1 b^0 + a^0 b^1 =$

$$= \binom{1}{0}a^1 b^0 + \binom{1}{1}a^0 b^1$$

ii ) Hipótesis $(a+b)^h = \sum_{k=0}^{h} \binom{h}{k} a^{h-k} b^k$

Tesis) $(a+b)^{h+1} = \sum_{k=0}^{h+1} \binom{h+1}{k} a^{h+1-k} b^k$

Demostración) Aplicando la definición de potenciación y la hipótesis inductiva, se tiene

$$(a+b)^{h+1} = (a+b) \,.\, (a+b)^h =$$

$$= (a+b) \,.\, \sum_{k=0}^{h} \binom{h}{k} a^{h-k} b^k$$

Por distributividad

$$(a+b)^{h+1} = a \sum_{k=0}^{h} \binom{h}{k} a^{h-k} b^k + b \sum_{k=0}^{h} \binom{h}{k} a^{h-k} b^k$$

Por 6.5.2. ii ) introducimos $a$ y $b$ en cada sumatoria

$$(a+b)^{h+1} = \sum_{k=0}^{h} \binom{h}{k} a^{h-k+1} b^k + \sum_{k=0}^{h} \binom{h}{k} a^{h-k} b^{k+1}$$

Efectuando operaciones

$$(a+b)^{h+1} = \binom{h}{0} a^{h+1} b^0 + \sum_{k=1}^{h} \binom{h}{k} a^{h-k+1} b^k +$$

$$+ \sum_{k=0}^{h-1} \binom{h}{k} a^{h-k} b^{k+1} + \binom{h}{h} a^0 b^{h+1}$$

Teniendo en cuenta que el índice de la sumatoria puede tomar cualquier nombre, en la segunda cambiamos $k$ por $j$

$$(a+b)^{h+1} = \binom{h}{0} a^{h+1} b^0 + \sum_{k=1}^{h} \binom{h}{k} a^{h-k+1} b^k + \sum_{j=0}^{h-1} \binom{h}{j} a^{h-j} b^{j+1} + \binom{h}{h} a^0 b^{h+1}$$

Para reducir ambas sumatorias hacemos $j = k-1 \Rightarrow k = j+1$, y sustituyendo en la misma sumatoria

$$(a+b)^{h+1} = \binom{h}{0} a^{h+1} b^0 + \sum_{k=1}^{h} \binom{h}{k} a^{h-k+1} b^k + \sum_{k=1}^{h} \binom{h}{k-1} a^{h-k+1} b^k + \binom{h}{h} a^0 b^{h+1}$$

Como $\binom{h}{0} = \binom{h+1}{0}$, y $\binom{h}{h} = \binom{h+1}{h+1}$

después de sustituir y aplicar 6.5.2 i ), nos queda

$$(a+b)^{h+1} = \binom{h+1}{0} a^{h+1} b^0 + \sum_{k=1}^{h} \left[\binom{h}{k} + \binom{h}{k-1}\right] a^{h-k+1} b^k + \binom{h+1}{h+1} a^0 b^{h+1}$$

Teniendo en cuenta por 6.7.2 ii ) que

$$\binom{h}{k} + \binom{h}{k-1} = \binom{h+1}{k} \quad \text{resulta}$$

$$(a+b)^{h+1} = \binom{h+1}{0} a^{h+1} b^0 + \sum_{k=1}^{h} \binom{h+1}{k} a^{h-k+1} b^k + \binom{h+1}{h+1} a^0 b^{h+1}$$

Es decir

$$(a+b)^{h+1} = \sum_{k=0}^{h+1} \binom{h+1}{k} a^{h+1-k} b^k$$

como se quería.

***Ejemplo 6-14.***

Desarrollar $(-x+2y)^5$.

Aplicamos la fórmula demostrada

$$(-x+2y)^5 = \binom{5}{0}(-x)^5(2y)^0 + \binom{5}{1}(-x)^4(2y)^1 + \binom{5}{2}(-x)^3(2y)^2 +$$

$$+ \binom{5}{3}(-x)^2(2y)^3 + \binom{5}{4}(-x)^1(2y)^4 + \binom{5}{5}(-x)^0(2y)^5 =$$

$$= -x^5 + 10x^4y - 40x^3y^2 + 80x^2y^3 - 80xy^4 + 32y^5$$

### 6.8.2. Observaciones

Sea

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}\,b^k$$

i ) El desarrollo de la potencia $n$-sima de un binomio tiene $n+1$ términos, según lo indica la variación de $k$, desde 0 hasta $n$.

ii ) Cada término del desarrollo tiene como coeficiente un número combinatorio de numerador igual al exponente del binomio, y el denominador es variable desde 0 hasta $n$.

iii) El exponente de $a$ es la diferencia entre el numerador y denominador, y el de $b$ es igual al denominador. Es decir, la suma de ambos exponentes es igual a $n$ para todos los términos.

iv) El término de lugar $h$ en el desarrollo, es

$$T_h = \binom{n}{h-1}a^{n-h+1}\,b^{h-1}$$

(v) Los términos equidistantes de los extremos tienen igual coeficiente, por ser números combinatorios de órdenes complementarios.

*Ejemplo*

Determinar la suma del 4º y 6º términos del desarrollo de

$$(2a-a^2)^8$$

Como

$$T_4 = \binom{8}{3}(2a)^5(-a^2)^3 = -\binom{8}{3}.\,32\,a^{11}$$

$$T_6 = \binom{8}{5}(2a)^3(-a^2)^5 = -\binom{8}{5}.\,8\,a^{13}$$

$$\Rightarrow T_4 + T_6 = -8\,.\binom{8}{3}(4a^{11} + a^{13})$$

***Ejemplo 6-16.***

a) Demostrar

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

Trasformamos la sumatoria en el desarrollo de la potencia de un binomio

$$\sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} \cdot 1^{i} = (1+1)^n = 2^n$$

b)
$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$$

Procediendo análogamente

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} (-1)^i = (1-1)^n = 0^n = 0$$

***Ejemplo 6-17.***

Determinar el término central del desarrollo de

$$\left(x^2 + \frac{1}{x}\right)^{2n} \qquad \text{con } x \neq 0$$

El número de términos es

$$2n + 1 = n + n + 1 = n + 1 + n$$

El término central está precedido por $n$ términos, y en consecuencia ocupa el lugar $(n+1)$. Se tiene

$$T_{n+1} = \binom{2n}{n} (x^2)^n \left(\frac{1}{x}\right)^n$$

$$T_{n+1} = \binom{2n}{n} x^{2n} \frac{1}{x^n}$$

Es decir

$$T_{n+1} = \binom{2n}{n} x^n$$

En cuanto al coeficiente

$$\binom{2n}{n} = \frac{(2n)!}{n!\,(2n-n)!} = \frac{(2n)!}{(n!)^2} =$$

$$= \frac{2n(2n-1)(2n-2)\ \dots\ [2n-(n-1)].\ n!}{(n!)^2} =$$

$$= \frac{2n(2n-1)(2n-2)\ \dots\ (n+1)}{n!}$$

***Ejemplo 6-18.***

Obtener el término de grado 14 del desarrollo de

$$(x^3 - 3\,x)^{10}$$

El desarrollo admite 11 términos y se trata de ubicar aquel en el cual el exponente de $x$ sea 14. Este término ocupa un lugar $h$, a determinar basándose en la condición anterior

$$\begin{aligned} \mathrm{T}_h &= \binom{10}{h-1}(x^3)^{10-h+1}(-3\,x)^{h-1} = \\ &= \binom{10}{h-1}x^{33-3h}(-3)^{h-1}\,x^{h-1} = \\ &= (-3)^{h-1}\binom{10}{h-1}x^{32-2h} \end{aligned}$$

Debe ser: $32 - 2\,h = 14 \Rightarrow 2\,h = 18 \Rightarrow h = 9$

Es decir, el 9º término tiene grado 14.

Lo calculamos

$$\mathrm{T}_9 = \binom{10}{8}\,x^3\,(-3\,x)^9 = -3^9 \,.\, 10\,x^{14}$$

***Ejemplo 6-19***

Desarrollar $\left(1 + \frac{1}{n}\right)^n$

Llegaremos a una expresión que se utiliza en la determinación del número $e$, en los cursos básicos de análisis.

$$\left(1 + \frac{1}{n}\right)^n = 1 + \binom{n}{1}\frac{1}{n} + \binom{n}{2}\left(\frac{1}{n}\right)^2 + \binom{n}{3}\left(\frac{1}{n}\right)^3 + $$

$$+ \ldots + \binom{n}{n-1}\left(\frac{1}{n}\right)^{n-1} + \binom{n}{n}\left(\frac{1}{n}\right)^n$$

Después de haber omitido las potencias de 1. Operando y utilizando la fórmula del ejemplo 6-13 iii), tenemos

$$\left(1 + \frac{1}{n}\right)^n = 1 + \cancel{n}\,.\,\frac{1}{\cancel{n}} + \frac{n\,(n-1)}{2!}\,\frac{1}{n^2} \;+$$

$$+ \frac{n\,(n-1)\,(n-2)}{3!}\,\frac{1}{n^3} + \ldots + \frac{n\,(n-1)\,(n-2)\ldots[n-(n-2)]}{(n-1)!}\,\frac{1}{n^{n-1}} +$$

$$+ \frac{n\,(n-1)\,(n-2)\,\ldots\,[n-(n-1)]}{n!}\,.\,\frac{1}{n^n}$$

A partir del tercer término dividimos cada factor del numerador por el factor $n$ que figura en cada denominador

$$\left(1+\frac{1}{n}\right)^n = 1+1+\frac{1}{2!}\cdot\frac{n-1}{n}+\frac{1}{3!}\ \frac{n-1}{n}\ \frac{n-2}{n}+$$
$$+\dots+\frac{1}{(n-1)!}\ \frac{n-1}{n}\ \frac{n-2}{n}\dots\frac{n-(n-2)}{n}+$$
$$+\frac{1}{n!}\ \frac{n-1}{n}\cdot\frac{n-2}{n}\dots\frac{n-(n-1)}{n}$$

Resulta

$$\left(1+\frac{1}{n}\right)^n = 2+\frac{1}{2!}\ \left(1-\frac{1}{n}\right)+\frac{1}{3!}\ \left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)+$$
$$+\dots+\frac{1}{(n-1)!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\dots\left(1-\frac{n-2}{n}\right)+$$
$$+\frac{1}{n!}\ \left(1-\frac{1}{n}\right)\cdot\left(1-\frac{2}{n}\right)\dots\left(1-\frac{n-2}{n}\right)\left(1-\frac{n-1}{n}\right)$$

*Ejemplo 6-20.*

Determinar $x \in \mathbf{R}$ de modo que la suma de los términos 3º y 8º del desarrollo de $\left(2x^3-\frac{1}{x}\right)^9$ sea igual a 0.

Debe verificarse

$$T_3 + T_8 = 0$$

O sea

$$\binom{9}{2}(2x^3)^7\left(-\frac{1}{x}\right)^2+\binom{9}{7}\ (2x^3)^2\left(-\frac{1}{x}\right)^7 = 0$$

Los números combinatorios son iguales y pueden cancelarse

$$2^7\cdot x^{21}\cdot\frac{1}{x^2}-2^2\,x^6\ \frac{1}{x^7}\ =\ 0$$

$$2^7\cdot x^{19}\ -2^2\cdot\frac{1}{x}=0$$

Multiplicando por $\frac{x}{2^2}$

$$2^5\cdot x^{20}-1=0$$

Resulta

$$x^{20} = \frac{1}{2^5}$$

Es decir

$$x = \pm \sqrt[20]{\frac{1}{2^5}} \quad \text{en } \mathbf{R}$$

Por distributividad y simplificación

$$x = \pm \frac{1}{\sqrt[4]{2}}$$

Racionalizando

$$x = \pm \frac{\sqrt[4]{8}}{2}$$

Ambos valores de $x$ satisfacen la condición dada.

## 6.9. FUNCIONES ENTRE INTERVALOS NATURALES INICIALES

A fin de tratar el tema de la Combinatoria simple y con repetición desde un punto de vista funcional, proponemos algunos conceptos y propiedades relativos a funciones cuyos dominio y codominio son conjuntos finitos, no vacíos y por consiguiente identificables, en cuanto a su cardinalidad, con intervalos naturales iniciales $I_n$ e $I_m$.

### 6.9.1. Aplicaciones inyectivas de $I_n$ en $I_m$ ($n \leqslant m$)

Sea el conjunto cuyos elementos son todas las aplicaciones inyectivas de $I_n$ en $I_m$, y que denotamos con

$$In\,(I_n\,, I_m) = \left\{ f : I_n \to I_m \,/ f \text{ es inyectiva} \right\}$$

Se necesita la restricción $n \leqslant m$, ya que en caso contrario habría dos elementos del dominio con la misma imagen en el codominio, y ninguna aplicación sería 1-1.

El elemento 1 de $I_n$ puede aplicarse sobre cualquiera de los $m$ elementos del codominio $I_m$, es decir, existen $m$ posibilidades para el $1 \in I_n$. Una vez asignada la imagen, para construir una función inyectiva, el $2 \in I_n$ admite $(m-1)$ imágenes posibles en $I_m$. Seleccionadas sendas imágenes para el 1 y el 2, se presentan $(m-2)$ posibilidades para la imagen de $3 \in I_n$. Suponiendo hecha la selección de imágenes para $1, 2, \ldots, n-1$, el elemento $n \in I_n$ puede proyectarse sobre cualquiera de los $m-(n-1)$ elementos restantes del codominio, y en consecuencia el número total de aplicaciones inyectivas de $I_n$ en $I_m$ es

$$m\,.\,(m-1)\,.\,(m-2)\,\ldots\,[m-(n-1)]$$

Es decir, el cardinal de $In(I_n, I_m)$ es igual al producto de $n$ factores decrecientes en una unidad, a partir de $m$.

Denotando tal número cardinal con el símbolo $V_{m,n}$, se tiene

$$V_{m,n} = m \cdot (m-1) \cdot (m-2) \ldots (m-n+1) \qquad (1)$$

Multiplicamos y dividimos el segundo miembro de esta expresión por

$$(m-n)(m-n-1) \ldots \ldots 2 \cdot 1 = (m-n)!$$

$$V_{m,n} = \frac{m \cdot (m-1) \cdot (m-2) \ldots (m-n+1) \cdot (m-n)!}{(m-n)!}$$

y resulta

$$V_{m,n} = \frac{m!}{(m-n)!} \qquad (2)$$

Demostraremos ahora esta fórmula por inducción sobre $n$.

i ) Si $n = 1$, entonces el número de funciones inyectivas de $I_1$ en $I_m$ es exactamente $m$, y se tiene

$$V_{m,1} = m = \frac{m \cdot (m-1)!}{(m-1)!} = \frac{m!}{(m-1)!}$$

ii ) Probaremos que si la fórmula (2) vale para $h$, también es válida para $h+1$.

Hipótesis) $$V_{m,h} = \frac{m!}{(m-h)!}$$

Tesis) $$V_{m,h+1} = \frac{m!}{[m-(h+1)]!}$$

Demostración) Supongamos definida una función inyectiva de $I_h$ en $I_m$. Si extendemos el dominio a $I_{h+1}$, el elemento agregado, $h+1$, puede hacerse corresponder con cualquiera de los $(m-h)$ elementos restantes del codominio. Es decir, cada función inyectiva de $I_h$ en $I_m$ origina $(m-h)$ funciones inyectivas de $I_{h+1}$ en $I_m$, y en consecuencia se tiene

$$V_{m,h+1} = V_{m,h} \cdot (m-h)$$

Usando la hipótesis inductiva llegamos a

$$V_{m,h+1} = \frac{m!}{(m-h)!} \cdot (m-h) = \frac{m!\,(m-h)}{(m-h) \cdot (m-h-1)!} = \frac{m!}{[m-(h+1)]!}$$

*Ejemplo 6-21.*

¿Cuántos números de tres cifras distintas pueden formarse con 1, 2, 3, 4?

Cada número pedido corresponde al conjunto imagen de una aplicación inyectiva (ya que no pueden repetirse) de $I_3$ en $I_4$. Es decir, existen tantos números de tres

cifras distintas elegidas entre 1, 2, 3 y 4 como funciones inyectivas de $I_3$ en $I_4$, y resulta

$$V_{4,3} = 4 \cdot 3 \cdot 2 = 24 \text{ según la fórmula (1)}$$

### 6.9.2. Relación de equivalencia en $In\,(I_n, I_m)$ $(n \leq m)$

***Definición***

Dos funciones inyectivas de $I_n$ en $I_m$ son equivalentes si y sólo si admiten el mismo conjunto imagen.

$$f \sim g \Leftrightarrow I(f) = I(g)$$

Esta definición caracteriza una relación de equivalencia en $In\,(I_n, I_m)$, como puede verificarse con facilidad.

De acuerdo con el teorema fundamental de las relaciones de equivalencia existe una partición del conjunto de las aplicaciones inyectivas de $I_n$ en $I_m$, en clases de equivalencia.

En el caso del ejemplo 6-21, las funciones

$$f = \{(1,1), (2,3), (3,4)\} \quad \text{y} \quad g = \{(1,3), (2,1), (3,4)\}$$

son equivalentes, ya que ambos conjuntos imágenes se identifican. A manera de ejemplo nos proponemos exhibir la partición de $In\,(I_n, I_m)$ con la siguiente simplificación:

Como todas las funciones inyectivas admiten el mismo dominio $I_3$ es suficiente, para caracterizarlas, dar el conjunto ordenado de sus imágenes. Así

134 corresponde a $f$

314 corresponde a $g$

Si consideramos como imagen a 213, se trata de la función inyectiva

$$\{(1,2), (2,1), (3,3)\}$$

Con este criterio, la partición de $In\,(I_3, I_4)$ es

| | | | |
|---|---|---|---|
| 123 | 124 | 134 | 234 |
| 132 | 142 | 143 | 243 |
| 213 | 214 | 314 | 324 |
| 231 | 241 | 341 | 342 |
| 312 | 412 | 413 | 423 |
| 321 | 421 | 431 | 432 |

En cada clase de equivalencia hay tantas funciones como aplicaciones inyectivas de $I_3$ en $I_3$, es decir, $3 \cdot 2 \cdot 1 = 3!$ elementos.

El número de clases de equivalencia es naturalmente igual al número total de

funciones inyectivas de $I_3$ en $I_4$, dividido por el número de elementos de cada clase, es decir

$$\frac{\frac{4!}{(4-3)!}}{3!} = \frac{4!}{3!\ (4-3)!} = \binom{4}{3}$$

Si denotamos con $C_{4,3}$ el número de clases de equivalencia se tiene

$$C_{4,3} = \binom{4}{3} = 4$$

En general, el número de clases de equivalencia determinado por la relación (1) en el conjunto de las funciones inyectivas de $I_n$ en $I_m$, está dado por

$$C_{m,n} = \binom{m}{n}$$

En efecto, sea $V_{m,n}$ el número de funciones inyectivas de $I_n$ en $I_m$, donde está definida la relación de equivalencia (1). En cada clase de equivalencia hay tantas funciones como aplicaciones inyectivas de $I_n$ en $I_n$, las que son, además, sobreyectivas, es decir, biyectivas. Este número es, precisamente

$$V_{n,n} = \frac{n!}{(n-n)!} = n!$$

El número de clases es, entonces

$$C_{m,n} = \frac{V_{m,n}}{n!} = \frac{m!}{n!\ (m-n)!} = \binom{m}{n}$$

### 6.9.3. Funciones estrictamente crecientes de $I_n$ en $I_m$ $(n \leq m)$

*Definición*

$f : I_n \to I_m$ es estrictamente creciente si y sólo si

$$x < y \Rightarrow f(x) < f(y)$$

La función $f$ del párrafo anterior es estrictamente creciente, pero $g$ no lo es.

Volviendo al ejemplo propuesto en 6.9.2., si elegimos un único elemento en cada clase de equivalencia, se lo puede tomar como representante de dicha clase. La elección natural está dada por la función estrictamente creciente que figura en cada clase, y se tiene

123 124 134 234

El número de clases de equivalencia está dado por el número de funciones estrictamente crecientes de $I_3$ en $I_4$. Realizando esta identificación de clases de equivalencia con funciones estrictamente crecientes, podemos decir que existen tantas clases como subconjuntos de 3 elementos pueden extraerse de $I_4$.

*Ejemplo 6-22.*

¿Cuántas comisiones de 3 personas pueden formarse con 4 personas? Rotulando a las cuatro personas con 1, 2, 3 y 4, las selecciones

123 132 213 231 312 321

corresponden a la misma comisión (se supone que no hay distinción de jerarquías), y la selección natural es 123. Esta corresponde a una función estrictamente creciente de $I_3$ en $I_4$, y en consecuencia el número total de comisiones es

$$C_{4,3} = \binom{4}{3} = \frac{V_{4,3}}{3!} = \frac{4 \cdot 3 \cdot 2}{3 \cdot 2 \cdot 1} = 4$$

*Ejemplo 6-23.*

¿Cuántos números de tres cifras distintas pueden formarse con las cifras 1, 2 y 3?

A la luz de lo que hemos visto en el ejemplo 6-21, se tienen tantos números como funciones inyectivas de $I_3$ en $I_3$, las cuales son, además, biyectivas.

Entonces dicho número es

$$V_{3,3} = 3! = 6$$

### 6.9.4. Funciones de $I_n$ en $I_m$

Sean $n$ y $m$ números naturales cualesquiera. Se presenta el problema de determinar el número de funciones de $I_n$ en $I_m$.

Es claro que, elegida una de las $m$ posibilidades para la elección de la imagen de $1 \in I_n$, para el 2 también se presentan $m$, ya que no hay restricciones de inyectividad. El número total de tales funciones, que denotamos con $V'_{m,n}$, es $\underbrace{m \cdot m \ldots m}_{n} = m^n$.

Demostramos, por inducción sobre $n$, la fórmula $V'_{m,n} = m^n$.

i ) Si $n = 1$, entonces se tienen $m$ funciones de $I_1$ en $I_m$, es decir

$V'_{m,1} = m = m^1$, con lo que la fórmula es válida en este caso.

ii ) Supongamos que se verifica para $n = h$, es decir $V'_{m,h} = m^h$. Debemos probar que $V'_{m,h+1} = m^{h+1}$.

Sea una función de $I_h$ en $I_m$; si el dominio es ahora $I_{h+1}$, entonces el elemento $h + 1$ puede aplicarse sobre cualquiera de los $m$ elementos del codominio. Podemos decir que cada aplicación de $I_h$ en $I_m$ caracteriza $m$ funciones de $I_{h+1}$ en $I_m$, y el número de éstas es

$$V'_{m,h+1} = m \cdot V'_{m,h}$$

Aplicando la hipótesis y la definición de potenciación, se tiene

$$V'_{m,h+1} = m \cdot m^h = m^{h+1}$$

***Ejemplo 6-24.***

¿Cuántos números de tres cifras pueden formarse con 1, 2, 3 y 4?

Como no hay restricciones en cuanto a que las cifras deban ser diferentes, los números 134, 143, 112, 222, etc., figuran entre los pedidos. Cada uno de ellos puede considerarse como el conjunto ordenado de las imágenes de una función de $I_3$ en $I_4$. En consecuencia existen tantos números de tres cifras formados con 1, 2, 3 y 4 como funciones de $I_3$ en $I_4$, es decir

$$V'_{4,3} = 4^3 = 64.$$

### 6.9.5. Funciones crecientes de $I_n$ en $I_m$

Sean $n$ y $m$ números naturales cualesquiera.

***Definición***

La función $f : I_n \to I_m$ es creciente si y sólo si

$$x < y \Rightarrow f(x) \leq f(y)$$

***Ejemplo 6-25.***

i ) Las imágenes de todas las funciones crecientes de $I_3$ en $I_4$ son

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 111 | 122 | 133 | 144 | 222 | 233 | 244 | 333 | 344 | 444 |
| 112 | 123 | 134 | | 223 | 234 | | 334 | | |
| 113 | 124 | | | 224 | | | | | |
| 114 | | | | | | | | | |

Hemos seguido una ley de formación a partir de 11, 12, 13, 14, 22, etcétera.

ii ) Las funciones crecientes de $I_3$ en $I_2$ tienen las imágenes

111 122 222
112

Llamando $C'_{m,n}$ al número de funciones crecientes de $I_n$ en $I_m$, se tiene, para los casos anteriores

$$C'_{4,3} = 20 \qquad C'_{2,3} = 4$$

Observamos que el número de funciones crecientes de $I_m$ en $I_n$ se identifica con el número de funciones estrictamente crecientes de $I_{m+n-1}$ en $I_n$, ya que

$$C'_{4,3} = C_{4+3-1,3} = C_{6,3} = \frac{6 \cdot 5 \cdot 4}{3!} = 20$$

$$C'_{2,3} = C_{2+3-1,3} = C_{4,3} = \frac{4 \cdot 3}{3!} = 4$$

**Teorema** El número de funciones crecientes de $I_n$ en $I_m$ es igual al de funciones estrictamente crecientes de $I_n$ en $I_{m+n-1}$.

Tesis) $C'_{m,n} = C_{m+n-1}$

Demostración) Sean A el conjunto de todas las funciones crecientes de $I_n$ en $I_m$, y B el conjunto de las funciones estrictamente crecientes de $I_n$ en $I_{m+n-1}$. Nuestro propósito es probar que $c(A) = c(B)$, es decir, que A y B son coordinables. Para esto es suficiente ver que existe una aplicación biyectiva de A en B.

Para definir tal aplicación hay que asignar a cada función de A una única función en B.

Sea $f \in A$. La imagen de $f$ es

$$f(1), f(2), \ldots, f(n)$$

tal que para todo $i = 1, 2, \ldots, n$ se verifica $1 \leqslant f(i) \leqslant m$ (1).

A expensas de $f$, definimos $g : I_n \to I_{m+n-1}$ mediante las asignaciones

$$(2)\begin{cases} g(1) = f(1) \\ g(2) = f(2) + 1 \\ g(3) = f(3) + 2 \\ \cdots\cdots\cdots \\ g(n) = f(n) + (n-1) \end{cases}$$

De este modo, los valores extremos que puede tomar $g$ son, de acuerdo con (1): 1 y $m + n - 1$. Además, teniendo en cuenta (1) y la definición de $g$, se verifica

$f \in A \Rightarrow f(1) \leqslant f(2)$, y como $0 < 1$, sumando resulta

$$f(1) + 0 < f(2) + 1 .$$

Es decir

$$f(1) < f(2) + 1 .$$

Luego

$$g(1) < g(2) .$$

Procediendo análogamente vale la proposición

$$1 \leqslant f(1) < f(2) + 1 < f(3) + 2 < \ldots < f(n) + (n-1) \leqslant m + n - 1$$

Es decir

$$1 \leqslant g(1) < g(2) < g(3) < \ldots < g(n) \leqslant m + n - 1$$

La asignación propuesta en (2) permite definir la aplicación

$$F: A \to \overset{*}{B} \text{ tal que } F(f) = g$$

Falta probar que F es biyectiva. Para ello estudiamos

i ) Inyectividad de F. Sean $f$ y $f'$ en A, tales que $F(f) = F(f')$, es decir, tales que $g = g'$. Esto significa que los conjuntos

$$\{f(1), f(2)+1, \ldots, f(n)+(n-1)\}$$
$$\{f'(1), f'(2)+1, \ldots, f'(n)+(n-1)\}$$

son iguales, y en consecuencia $f(i) = f'(i)$ cualquiera que sea $i = 1, 2, \ldots, n$. Resulta entonces $f = f'$; y por lo tanto, F es inyectiva.

ii ) Sobreyectividad de F. Sea $g \in B$.

Entonces $g: I_n \to I_{m+n-1}$ es estrictamente creciente, y se tiene

$$1 \leqslant g(1) < g(2) < g(3) < \ldots < g(n) \leqslant m + n - 1$$

Ahora bien, $g(2) > g(1) \Rightarrow g(2) - g(1) > 0 \Rightarrow g(2) - g(1) \geqslant 1$, ya que todo número natural es mayor o igual que 1. Resulta $g(1) \leqslant g(2) - 1$, y procediendo análogamente tenemos

$$1 \leqslant g(1) \leqslant g(2) - 1 \leqslant g(3) - 2 \leqslant \ldots \leqslant g(n) - (n-1) \leqslant m$$

Esta situación permite definir la función $f: I_n \to I_m$, creciente, con la asignación

$$f(i) = g(i) - (i-1)$$

Entonces, cualquiera que sea $g \in B$, existe $f \in A$ tal que $F(f) = g$.

Las partes i ) y ii ) prueban que F es biyectiva, es decir, $A \sim B$, y en términos de números cardinales vale la fórmula

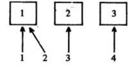
$$C'_{m,n} = C_{m+n-1} = \binom{m+n-1}{n}$$

***Ejemplo 6-26.***

¿De cuántas maneras pueden entrar 4 alumnos en 3 aulas, si no se hace distinción de personas?

Rotulemos a los alumnos con: 1, 2, 3, y 4, y las aulas con: 1, 2 y 3. Es claro que una distribución de las cuatro personas en las tres aulas está asociada a una función de $I_4$ en $I_3$; por no haber distinción de personas, el hecho de que entren dos personas en el aula 1, una en el aula 2 y otra en el aula 3 está dado por una función cuya imagen es cualquiera de las siguientes:

1123
3121
3211, etc.



Al no haber distinción, estas distribuciones de cuatro alumnos en tres aulas son la misma. De ellas elegimos naturalmente la que define a una función creciente de $I_4$ en $I_3$ es decir 1123.

Otra distribución distinta es, por ejemplo, 1113, que significa: tres alumnos entraron en el aula 1 y el cuarto en el aula 3.

De modo que existen tantas distribuciones posibles de 4 personas en 3 aulas, sin distinción de las personas, como funciones crecientes de $I_4$ en $I_3$, es decir

$$C'_{3,4} = C_{3+4-1,4} = C_{6,4} = \binom{6}{4} = \frac{6\,.\,5\,.\,3\,.\,4}{4\,.\,3\,.\,2\,.\,1} = 15$$

### 6.9.6. Aplicaciones estrictamente crecientes por trazos de $I_m$ en $I_m$

Sean los números naturales $m$, $m_1$, $m_2, \ldots, m_n$, tales que

$$m = m_1 + m_2 + \ldots + m_n = \sum_{i=1}^{n} m_i \qquad (1)$$

Asociada a la descomposición (1), queda especificada la siguiente partición de $I_m$ en intervalos naturales cerrados

$$I_m = [1\,, m_1] + [m_1 + 1\,, m_1 + m_2] + [m_1 + m_2 + 1\,, m_1 + m_2 + m_3] + \ldots + \left[\sum_{i=1}^{k-1} m_i + 1\,, m\right] \qquad (2)$$

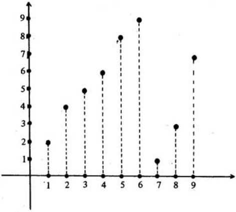
donde el signo + denota una unión disjunta.

i ) *Definición*

La función $f : I_m \to I_m$ es estrictamente creciente por trazos, respecto de la partición (2), si y sólo si es estrictamente creciente su restricción a cada subconjunto de la partición.

*Ejemplo 6-27.*

En correspondencia con la descomposición $9 = 2 + 4 + 3$ se tiene la siguiente función estrictamente creciente por trazos de $I_9$ en $I_9$.



Se tiene aquí la partición $I_9 = [1\,,2] + [3\,,6] + [7\,,9]$, es decir

$$I_9 = \{1\,,2\} + \{3\,,4\,,5\,,6\} + \{7\,,8\,,9\}$$

Y la restricción de $f$ a cada elemento de la partición es estrictamente creciente.

***Ejemplo 6-28.***

Determinamos el número de aplicaciones estrictamente crecientes por trazos de $I_7$ en $I_7$, respecto de la partición de $I_7$ asociada a la descomposición $7 = 3 + 4$. De acuerdo con la definición, la restricción de cada una de las funciones a los subconjuntos $I_3$ e $I_4$ debe ser estrictamente creciente.

Se sabe que el número de aplicaciones estrictamente crecientes de $I_3$ en $I_7$ es

$$C_{7,3} = \binom{7}{3}$$

Además, es claro que cada función estrictamente creciente de $I_3$ en $I_7$ define unívocamente una función estrictamente creciente de 4, 5, 6, 7 en $I_7$. Por ejemplo, si $g : I_3 \to I_7$ está definida por

$$g(1) = 2 \qquad g(2) = 5 \qquad g(3) = 7$$

queda determinada $h : \{4\,,5\,,6\,,7\} \to I_7$ estrictamente creciente y única, a saber

$$h(4) = 1 \qquad h(5) = 3 \qquad h(6) = 4 \qquad h(7) = 6$$

En consecuencia, el número de aplicaciones estrictamente crecientes por trazos de $I_7$ en $I_7$ es el de funciones estrictamente crecientes de $I_3$ en $I_7$, que denotamos mediante

$$P_7^{3,4} = \binom{7}{3} = \frac{7!}{3!\,4!}$$

En el caso del ejemplo 6-27, tal número es

$$P_9^{2,3,4} = \frac{9!}{2!\,3!\,4!}$$

ii) **Propiedad.** El número de aplicaciones estrictamente crecientes por trazos de $I_m$ en $I_m$, respecto de la partición (2), está dado por

$$P_m^{m_1, m_2, \ldots, m_n} = \frac{m!}{m_1!\, m_2! \ldots m_n!}$$

Para cada $m$ fijo hacemos inducción sobre el número $n$ de elementos de la partición de $I_m$.

a) Si $n = 1$, entonces la partición tiene como único elemento $I_m$, y la única función estrictamente creciente de $I_m$ en $I_m$ lo es estrictamente creciente por trazos, es decir

$$P_m^{m_1} = 1 = \frac{m!}{m!} = \frac{m!}{m_1!} \qquad \text{ya que} \quad m = m_1$$

b) Suponemos que la fórmula es válida para $n = h$, y demostramos su validez para $n = h + 1$.

Cada función estrictamente creciente por trazos de $I_{m-m_{h+1}}$ en sí mismo determina $C_{m,m_{h+1}}$ funciones estrictamente crecientes por trazos de $I_m$ en $I_m$, respecto de la partición asociada a la descomposición

$$m = m_1 + m_2 + \ldots + m_{h+1}$$

Entonces

$$P_m^{m_1, m_2, \ldots, m_{h+1}} = P_{m-m_{h+1}}^{m_1, m_2, \ldots, m_h} \cdot C_{m, m_{h+1}}$$

Aplicando la hipótesis inductiva, se tiene

$$P_m^{m_1, m_2, \ldots, m_{h+1}} = \frac{(m - m_{h+1})!}{m_1!\, m_2! \ldots m_h!} \cdot \frac{m!}{m_{h+1}!\,(m - m_{h+1})!}$$

Es decir

$$P_m^{m_1, m_2, \ldots, m_{h+1}} = \frac{m!}{m_1!\, m_2! \ldots m_{h+1}!}$$

*Ejemplo 6-29.*

¿Cuántos números distintos pueden formarse permutando las cifras del número 112223333?

Cada número que resulte de intercambiar las cifras de 112223333 define una aplicación estrictamente creciente por trazos de $I_9$ en $I_9$, y recíprocamente. Así, por ejemplo, el número 133221323 determina la aplicación de $I_9$ en $I_9$, asociada a la partición correspondiente a la descomposición $9 = 2 + 3 + 4$:

$$f(1) = 1 \quad f(2) = 6 \quad f(3) = 4 \quad f(4) = 5 \quad f(5) = 8$$

$$f(6) = 2 \quad f(7) = 3 \quad f(8) = 7 \quad f(9) = 9$$

La manera de determinarla es la siguiente: a cada elemento del dominio le asignamos como imagen, respecto de la partición dada, el lugar que ocupa en el número propuesto.

Recíprocamente, a toda función estrictamente creciente por trazos respecto de la partición, le corresponde un número que se deduce del dado, intercambiando las cifras. Así, si $f: I_9 \to I_9$ es tal que

$$f(1) = 2 \quad f(2) = 9 \quad f(3) = 5 \quad f(4) = 6 \quad f(5) = 7$$

$$f(6) = 1 \quad f(7) = 3 \quad f(8) = 4 \quad f(9) = 8$$

y el número resultante es 313322231.

Entonces el número total de números pedidos es igual al de funciones estrictamente crecientes por trazos de $I_9$ en $I_9$, respecto de la partición dada, es decir

$$P_9^{2,3,4} = \frac{9!}{2!\,3!\,4!} = \frac{9 \,.\, 8 \,.\, 7 \,.\, 6 \,.\, 5 \,.\, 4!}{1 \,.\, 2 \,.\, 1 \,.\, 2 \,.\, 3 \,.\, 4!} = 9 \,.\, 4 \,.\, 7 \,.\, 5 = 1260$$

## 6.10. COMBINATORIA SIMPLE Y CON REPETICION

### 6.10.1. Concepto

Identificando un conjunto finito y no vacío con un intervalo natural inicial, respecto de la coordinabilidad, la respuesta a la determinación del número cardinal de ciertos subconjuntos del mismo puede lograrse a la luz de cierto tipo de funciones entre intervalos naturales iniciales, ya estudiadas en 6.9. Los problemas que se presentan dependen del tipo de función que pueda diagnosticarse en relación con el problema, y son los seis que se tratan a continuación.

### 6.10.2. Variaciones simples de $m$ elementos de orden $n$. ($n \leqslant m$)

***Definición***

Variaciones simples de $m$ elementos de orden $n$, o variaciones $n$-arias de $m$ elementos, son todas las funciones inyectivas de $I_n$ en $I_m$.

Como todas las funciones inyectivas de $I_n$ en $I_m$ tienen el mismo dominio $I_n$, cualquier variación simple queda determinada por las segundas componentes de los pares ordenados correspondientes a la función. Desde este punto de vista, toda variación $n$-aria de $m$ elementos es un subconjunto ordenado de $n$ elementos de $I_m$. Es claro que la inyectividad exige que no se repitan elementos en la imagen, es decir, dos variaciones simples son distintas si difieren en algún elemento, o bien, si constan de los mismos, deben diferir en el orden.

De acuerdo con 6.9.1., su número está dado por la fórmula

$$V_{m,n} = \frac{m!}{(m-n)!} = m \,.\, (m-1) \,.\, (m-2) \ldots (m-n+1)$$

### 6.10.3. Permutaciones de $n$ elementos

***Definición***

Permutaciones de $n$ elementos son todas las funciones biyectivas de $I_n$ en $I_n$.

Como toda función biyectiva de $I_n$ en $I_n$ es inyectiva, se tiene un caso particular de variaciones simples, donde $m = n$.

Teniendo en cuenta el conjunto imagen, cada permutación de $n$ elementos es un conjunto estrictamente ordenado de $I_n$. Su número, de acuerdo con 6.9.1., está dado por la fórmula

$$P_n = V_{n,n} = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

Al decir permutaciones de $n$ elementos se debe entender que son simples, en el sentido de que no hay repetición, por la inyectividad.

### 6.10.4. Combinaciones simples de $m$ elementos de orden $n$. $(n \leqslant m)$

***Definición***

Combinaciones simples de $m$ elementos de orden $n$, o combinaciones $n$-arias de $m$ elementos, son todas las aplicaciones estrictamente crecientes de $I_n$ en $I_m$.

Una tal aplicación estrictamente creciente identifica un subconjunto de $n$ elementos de $I_m$, de modo único. Al mismo concepto puede llegarse en virtud de la relación de equivalencia definida en el conjunto de las funciones inyectivas de $I_n$ en $I_m$, de acuerdo con 6.9.2.

El número de combinaciones simples está dado por

$$C_{m,n} = \binom{m}{n} = \frac{V_{m,n}}{P_n}$$

### 6.10.5. Variaciones con repetición de $m$ elementos de orden $n$

***Definición***

Variaciones con repetición de $m$ elementos de orden $n$ son todas las funciones de $I_n$ en $I_m$.

En este caso no existen restricciones de $n$ respecto de $m$. Identificando cada variación con repetición con el correspondiente conjunto ordenado de las imágenes, ocurre que cada una es una $n$-upla de elementos de $I_m$. Su número está dado, de acuerdo con 6.9.4., por

$$V'_{m,n} = m^n$$

### 6.10.6. Combinaciones con repetición de $m$ elementos de orden $n$.

***Definición***

Combinaciones con repetición de $m$ elementos de orden $n$, son todas las funciones crecientes de $I_n$ en $I_m$.

En este caso, $m$ y $n$ son números naturales cualesquiera.

De acuerdo con 6.9.5., su número está dado por la fórmula

$$C'_{m,n} = C_{m+n-1,n} = \binom{m+n-1}{n}$$

### 6.10.7. Permutaciones con repetición

En muchas situaciones, los elementos de un conjunto están clasificados en tipos; digamos, por ejemplo, un conjunto de 9 libros, entre los cuales hay 2 de álgebra, 3 de geometría y 4 de filosofía. En cada caso se supone que son del mismo autor, edición, etc., es decir, indistinguibles. Un problema de interés consiste en la determinación de las distintas maneras según las cuales pueden ordenarse dichos libros en un estante.

Una ordenación posible es GAFAFGFFG. Es claro que si se permutan entre sí dos libros de filosofía, el ordenamiento es el mismo. Una distribución distinta de los 9 libros en el estante puede lograrse si se permutan libros de distinto tipo. Ahora bien, si rotulamos los libros asignando el 1 a los de álgebra, el 2 a los de geometría y el 3 a los de filosofía, la ordenación propuesta es

213132332

El problema consiste en determinar cuántos números pueden obtenerse intercambiando las cifras del propuesto, lo que se identifica con el número de aplicaciones estrictamente crecientes por trazos de $I_9$ en $I_9$, respecto de la partición asociada a la descomposición $9 = 2 + 3 + 4$. Tales aplicaciones se llaman permutaciones con repetición de 9 elementos, entre los cuales hay 2 del tipo A, 3 del tipo G y 4 del tipo F.

***Definición***

Permutaciones con repetición de $m$ elementos, entre los cuales hay $m_i$ del tipo $A_i$ $(i = 1, 2, \ldots, n)$, siendo $m = m_1 + m_2 + \ldots + m_n$ (1) son todas las aplicaciones estrictamente crecientes por trazos de $I_m$ en $I_m$, asociadas a la partición de $I_m^-$ correspondiente a la descomposición (1).

Según 6.9.6. ii ), su número es

$$P_m^{m_1, m_2, \ldots, m_n} = \frac{m!}{m_1!\, m_2! \ldots m_n!}$$

*Ejemplo 6-30.*

Seis personas viajan en un vehículo que tiene 10 paradas. ¿De cuántas maneras pueden bajarse en los siguientes casos?

i ) Si a lo sumo baja una persona por parada.

ii ) Sin restricciones.

En ambos casos, considerar la situación con distinción y sin distinción de personas.

Observamos que cada distribución de las 6 personas en las 10 paradas define una función de $I_6$ en $I_{10}$. Así, 122279 indica esta situación: una persona desciende en la primera parada, tres en la segunda, una en la séptima y una en la novena.

i ) A lo sumo baja una persona por parada.

Significa que personas distintas bajan en paradas distintas, y, si se hace distinción de personas, distribuciones como 134679 y 371496 son diferentes. Cada distribución de las 6 personas en las 10 paradas, con distinción de personas, define una función inyectiva de $I_6$ en $I_{10}$ y, en consecuencia, el número total es el de variaciones simples de 10 elementos de orden 6

$$V_{10,6} = 10 \,.\, 9 \,.\, 8 \,.\, 7 \,.\, 6 \,.\, 5$$

Si no se hace distinción de personas, las distribuciones 134679 y 371496 corresponden a la misma situación y se selecciona la que está asociada a una función estrictamente creciente de $I_6$ en $I_{10}$ En consecuencia, si no se hace distinción de personas, hay tantas distribuciones como combinaciones simples de 10 elementos de orden 6, es decir

$$C_{10,6} = \frac{V_{10,6}}{6!}$$

ii ) Sin restricciones.

En este caso puede bajarse más de una persona por parada, y, si se hace distinción de personas, cada distribución define una función de $I_6$ en $I_{10}$; es claro que se trata de las variaciones con repetición de 10 elementos de orden 6, y su número es

$$V'_{10,6} = 10^6$$

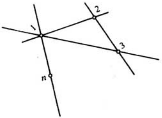
Si hay distinción de personas, 122279 y 721229 corresponden a situaciones diferentes. Pero si no se hace distinción de personas definen la misma distribución, y se elige la que corresponde a una función creciente de $I_6$ en $I_{10}$. El número total, en este caso, es el de combinaciones con repetición de 10 elementos de orden 6, es decir

$$C'_{10,6} = C_{10+6-1,6} = C_{15,6} = \frac{V_{15,6}}{6!}$$

***Ejemplo 6-31.***

¿Cuántas diagonales tiene un polígono convexo de $n$ lados?

El número de vértices es $n$, y, por definición, tres cualesquiera no están alineados. En consecuencia, cada par de vértices determina una recta.




El número total de rectas distintas está dado por el número de funciones estrictamente crecientes de $I_2$ en $I_n$, ya que, por ejemplo, las rectas 13 y 31 son la misma. Entre estas rectas figuran los lados y las diagonales. En consecuencia, el número de diagonales está dado por

$$C_{n,2} - n = \frac{n(n-1)}{2} - n = \frac{n^2 - 3n}{2}$$

***Ejemplo 6-32.***

¿De cuántas maneras pueden alinearse 10 personas, si tres de ellas han de estar juntas?

Una posible formación de las 10 personas es

$$\overset{\frown}{a_1\, a_2\, a_3}\, a_4\, a_5 \ldots a_{10}$$

Si no se especificaran condiciones, el número total sería el de funciones biyectivas de $I_{10}$ en $I_{10}$, es decir, $P_{10} = 10!$

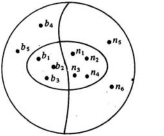
Sin pérdida de generalidad, podemos suponer que las tres primeras permanecen

juntas, y en primera instancia pueden considerarse como un solo objeto, con lo que el número total se reduce a 8, y se tienen $P_8$ arreglos distintos. Ahora bien, en cada uno de éstos, las tres personas que están juntas pueden permutarse entre sí, originando $P_3$ alineaciones diferentes. Entonces el número total es

$$P_8 \cdot P_3 = 8!\ 3!$$

***Ejemplo 6-33.***

En una urna hay 5 bolillas blancas y 6 bolillas negras numeradas. Se extraen muestras de tamaño 7. ¿Cuántas de tales muestras pueden extraerse? ¿En cuántas de ellas figuran exactamente 3 bolillas blancas?




i ) El experimento consiste en extraer al azar 7 bolillas de la urna, sin reposición. Es decir, se extraen una por una y no se reintegran hasta completar las siete. Dos muestras como

$$b_1\ b_2\ n_2\ n_3\ n_4\ n_5\ n_6\ b_3 \qquad n_3\ b_3\ n_6\ n_4\ n_5\ b_2\ b_1$$

son la misma, y existen tantas como subconjuntos de 7 elementos pueden formarse con 11 dados, es decir

$$C_{11,7} = C_{11,4} = \frac{V_{11,4}}{4!} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{4 \cdot 3 \cdot 2 \cdot 1} = 330$$

ii ) Consideremos ahora las 330 muestras aleatorias de tamaño 7 que pueden obtenerse. Estamos interesados en saber cuántas de tales muestras contienen exactamente 3 bolillas blancas.

Hay $C_{5,3}$ maneras de elegir 3 bolillas blancas entre las 5 que existen. Por cada una de estas posibilidades se presentan $C_{6,4}$ maneras de seleccionar 4 bolillas negras entre las 6 que hay. En consecuencia, el número total de muestras que tienen exactamente 3 bolillas blancas es

$$C_{5,3} \cdot C_{6,4} = \frac{5 \cdot 4 \cdot 3}{3 \cdot 2 \cdot 1} \cdot \frac{6 \cdot 5 \cdot 4 \cdot 3}{4 \cdot 3 \cdot 2 \cdot 1} = 150$$

***Ejemplo 6-34.***

Hay tres tipos de medallas: 3 de oro, 2 de plata y 4 de cobre. ¿De cuántas maneras pueden distribuirse entre 9 personas, si a cada persona le corresponde una y sólo una?

Cada distribución de las 9 medallas entre las 9 personas define una aplicación estrictamente creciente por trazos de $I_9$ en $I_9$, respecto de la partición asociada a la descomposición $9 = 3 + 2 + 4$. Se trata, entonces, de las permutaciones con repetición de 9 elementos, entre los cuales hay 3 del tipo 0, 2 del tipo P y 4 del tipo C, y su número es

$$P_9^{3,2,4} = \frac{9!}{3!\,2!\,4!} = 1260$$

***Ejemplo 6-35.***

¿Cuántos términos tiene un polinomio completo y homogéneo de grado 2 con 3 variables?

Sean éstas $x_1$, $x_2$ y $x_3$. Como el polinomio es homogéneo, todos los términos son de grado 2. Ahora bien, cada función creciente de $I_2$ en $I_3$ determina uno de los términos del polinomio, ya que las imágenes $x_1x_3$ y $x_3x_1$ corresponden al mismo término, y se considera la que es creciente.

El número total es el de combinaciones con repetición de 3 elementos de orden 2, es decir

$$C'_{3,2} = C_{3+2-1,2} = C_{4,2} = \frac{4\,.\,3}{2} = 6$$

El polinomio puede escribirse

$$P(x_1, x_2, x_3) = a_{11}\,x_1^2 + a_{22}\,x_2^2 + a_{33}\,x_3^2 + a_{12}\,x_1\,x_2 + a_{13}\,x_1\,x_3 + a_{23}\,x_2\,x_3$$

## TRABAJO PRACTICO VI

***6-36.*** **Demostrar por inducción completa**

1. $\sum_{i=0}^{n-1} x^i = \dfrac{1-x^n}{1-x}$ si $x \neq 1$

2. $\sum_{i=1}^{n} \dfrac{i}{2^i} = 2 - \dfrac{n+2}{2^n}$

3. $\sum_{i=1}^{n} i^2 = \dfrac{n(n+1)(2n+1)}{6}$

4. $\sum_{i=1}^{n} i(n-i) = \frac{n}{6}(n^2-1)$

5. $\sum_{i=1}^{n} 3^i = \dfrac{3}{2}(3^n-1)$

6. $\sum_{i=1}^{n} \left(\dfrac{2}{3}\right)^i = 2 - \dfrac{2^{n+1}}{3^n}$

7. $\alpha^n - 1 \geqslant n(\alpha - 1)$ si $\alpha > 1$

8. $(1+x)^n \geqslant 1 + nx$ si $x > 0$

9. $\sum_{i=1}^{n} \dfrac{1}{2^i} = 1 - \dfrac{1}{2^n}$

10. $3 \mid 10^{n+1} + 10^n + 1$

11. $2 \mid n^2 + n$

12. $3 \mid 8^n - 5^n$

13. $a^n - b^n = \alpha(a-b)$

14. $\sum_{i=1}^{n} i \,.\, i! = (n+1)! - 1$

15. $\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2$

*6-37.* Sean $x_1, x_2, \ldots, x_n$ números reales.
Demostrar que la suma de sus desvíos respecto del promedio es 0, es decir

$$\sum_{i=1}^{n} (x_i - \bar{x}) = 0$$

*6-38.* Demostrar que

$$\left(\sum_{i=1}^{n} x_i\right)^2 = \sum_{i=1}^{n} x_i^2 + \sum_{i \neq j}^{n} x_i x_j$$

*6-39.* Sabiendo que $x_1, x_2, \ldots, x_{10}$ son tales que

$$\sum_{i=1}^{10} x_i^2 = 100 \quad \text{y} \quad \bar{x} = -20, \quad \text{calcular}$$

$$\sum_{i=1}^{10} (x_i - 2)^2$$

*6-40.* Demostrar

i ) $2\,n! - (n-1)(n-1)! = n! + (n-1)!$

ii ) $\dfrac{n}{(n+1)!} = \dfrac{1}{n!} - \dfrac{1}{(n+1)!}$

*6-41.* Hallar $x$ sabiendo que

$$\binom{7}{x^2 - x} = \binom{7}{2x - 2}$$

*6-42.* Desarrollar las siguientes potencias

i ) $\left(-2a^2 + \dfrac{1}{a}\right)^6$

ii ) $(\sqrt{x} + \sqrt{y})^4$

*6-43.* i ) Sabiendo que $p + q = 1$, calcular

$$\sum_{k=0}^{n} \binom{n}{k} p^{n-k} q^k$$

ii ) Calcular $\sum_{k=0}^{n} t^k \binom{n}{k} \dfrac{1}{3^k} \left(\dfrac{2}{3}\right)^{n-k}$

*6-44.* Hallar la suma de los términos 5º y 7º del desarrollo de $(-2x + x^2)^{10}$

*6-45.* Determinar $x$ sabiendo que el término central del desarrollo de $\left(x + \dfrac{1}{2}\right)^8$ vale $\binom{8}{4}$.

*6-46.* Sea $\left(-2x+\frac{3}{2}\right)^7$ Determinar $x$ sabiendo que $T_3 + T_6 = 0$.

*6-47.* Hallar el término de grado 5 del desarrollo de $\left(x^2-\frac{1}{x}\right)^{10}$

*6-48* Hallar los términos de grado natural del desarrollo de $\left(x+\frac{1}{x^2}\right)^{15}$

*6-49.* ¿De cuántas maneras se pueden colocar 12 libros en un estante, si tres de ellos deben estar juntos?

*6-50.* ¿De cuántas maneras se pueden alinear 10 personas, sabiendo que dos de ellas no pueden estar juntas?

*6-51.* Calcular la suma de todos los números de 4 cifras no repetidos que pueden formarse con 1, 2, 3 y 4.

*6-52.* ¿Cuántas distribuciones circulares pueden formarse con 6 personas?

*6-53.* Ocho puntos del plano son tales que 3 cualesquiera no están alineados, salvo 4 de ellos que sí lo están. ¿Cuántas rectas determinan?

*6-54.* ¿Cuántas comisiones de 6 personas pueden formarse con 8 varones y 9 mujeres, sabiendo que al menos un varón integra cada comisión?

*6-55.* ¿De cuántas maneras se pueden distribuir 100 botellas de leche entre 10 comercios?

*6-56.* ¿Cuántos números de tres cifras distintas pueden formarse con 0, 1, 2, 3, 4 y 5?

*6-57.* ¿Cuántos números de tres cifras pueden formarse con 0, 1, 2, 3, 4 y 5?

*6-58.* De un mazo de naipes franceses (52 cartas) se extraen cinco cartas sin reposición. ¿De cuántas maneras pueden obtenerse exactamente dos ases?

*6-59.* Entre 36 cartas hay 4 ases. Se retiran tres cartas sin reposición. ¿Cuántas colecciones de tres cartas contienen exactamente 2 ases?

*6-60.* ¿En cuántos números de $k$ cifras elegidas al azar entre 1, 2, 3, . . . , 9, aparece exactamente 4 veces el número 1? $(k \geqslant 4)$

*6-61.* Se consideran $n$ personas alineadas al azar. ¿En cuántos, de dichos arreglos, hay exactamente $k$ personas entre dos determinadas?

*6-62.* ¿Cuántos polígonos determinan 10 puntos del plano, sabiendo que 3 cualesquiera no están alineados?

*6-63.* ¿De cuántas maneras pueden alinearse 5 varones y 5 mujeres de modo que aparezcan alternados?

*6-64.* ¿Cuántas $n$-uplas pueden formarse con los números 1, 2 y 3?
¿En cuántas aparece exactamente $k$ veces el 1?

*6-65.* Determinar el número de pronósticos posibles que corresponden a una fecha de los 13 partidos del juego llamado Prode. En cada partido puede apostarse a local, empate o visitante. ¿Cuántos de tales pronósticos tienen $k$ aciertos?

*6-66.* Demostrar que todo subconjunto infinito de un conjunto numerable es numerable.

*6-67.* Demostrar que la unión de un número finito de conjuntos numerables y disjuntos dos a dos es numerable.

*6-68.* Doce alumnos cursan una asignatura que se dicta en 4 horarios distintos. ¿De cuántas maneras pueden distribuirse los 12 alumnos en los 4 horarios? ¿Cuántas distribuciones determinan el mismo número de estudiantes en los 4 horarios?

*6-69.* Una persona apuesta 10 \$ en una carrera en la que intervienen 5 caballos. ¿Cuántas apuestas distintas puede hacer si cada vale cuesta 2 \$ ?

*6-70.* Para formar un compuesto se dispone de 6 sustancias del tipo A y de 8 del tipo B. El compuesto requiere 3 del primer tipo y 4 del segundo. ¿De cuántas maneras puede realizarse la experiencia en los siguientes casos?

i ) Sin restricciones.
ii ) Una sustancia determinada del tipo A debe ser incluida.
iii) Dos sustancias determinadas del tipo B no pueden incluirse.

Capítulo 7

# SISTEMAS AXIOMATICOS

## 7.1. INTRODUCCION

El desarrollo de la matemática actual es principalmente abstracto y se realiza, en gran parte, por la vía de los sistemas axiomáticos, cuyo concepto se expondrá en el presente capítulo. Este punto de vista representa el avance natural del desarrollo científico, entronca los casos particulares y concretos en situaciones generales de las cuales aquéllos se derivan, y esencialmente permite conocer mejor lo que antes se sabía de un modo fragmentario. Como ejemplo de sistema axiomático se desarrollan el álgebra de Boole y una introducción al sistema axiomático de Peano que conduce al estudio del número natural. Finalmente se presentan las estructuras algebraicas de monoide y semigrupo.

## 7.2. SISTEMAS AXIOMATICOS

### 7.2.1. Concepto

Un sistema axiomático, en matemática, consiste en los siguientes objetos:

i ) *términos primitivos* constituidos por elementos, conjuntos o relaciones, cuya naturaleza no queda especificada de antemano.

ii ) *axiomas*, que son funciones proposicionales cuantificadas, relativas a las variables que representan a los términos primitivos; es decir, son propiedades a las que deben satisfacer dichos términos primitivos. Los axiomas definen implícitamente a éstos.

iii) *definiciones* de todos los términos no primitivos.

iv) *teoremas*, es decir, propiedades que se deducen de los axiomas.

Anexada al sistema axiomático se admite la lógica bivalente, con cuyas leyes es posible demostrar los teoremas de la teoría.

Cuando se sustituyen las variables o términos primitivos por significados concretos, se tiene una interpretación del sistema axiomático; si esta interpretación es tal que los

axiomas se convierten en proposiciones verdaderas, entonces se tiene un modelo del sistema axiomático. En este caso, todo lo demostrado en abstracto en el sistema es válido para el modelo, y nada hay que probar en particular.

*Ejemplo 7-1.*

Consideramos el siguiente sistema axiomático.

i ) *términos primitivos.* Un conjunto A, y una relación $R$ definida en A, es decir, $R \subset A \times A$.

No se especifica aquí cuál es el conjunto ni se define la relación.

ii ) *axiomas:*

$A_1$ : $R$ es reflexiva en A
$A_2$ : $R$ es antisimétrica en A
$A_3$ : $R$ es transitiva en A
Los tres axiomas pueden resumirse en el siguiente: $R$ es una relación de orden amplio en A.

iii) *definición:* en A se considera la relación $S$, tal que

$$(a\,,\,b) \in S \Leftrightarrow (b\,,\,a) \in R$$

iv) *teoremas.* Demostramos la siguiente propiedad relativa a $S$:

$S$ es reflexiva en A.

$$\forall a : a \in A \Rightarrow (a\,,\,a) \in R \quad \text{por } A_1$$

$$(a\,,\,a) \in R \Rightarrow (a\,,\,a) \in S \quad \text{por iii)}$$

Entonces, por la ley del silogismo hipotético, resulta

$\forall a : a \in A \Rightarrow (a\,,\,a) \in S$ y en consecuencia, $S$ es reflexiva en A.

Con procedimiento análogo, se demuestra que $S$ es antisimétrica y transitiva en A. Esto significa que la relación $S$, inversa de $R$, determina un orden amplio en A.

Damos las siguientes interpretaciones para este sistema axiomático:

a) Si A es el conjunto de los números reales, y $R$ es la relación de "menor o igual", se verifican $A_1$, $A_2$ y $A_3$. La relación $S$ es, en este caso, la de "mayor o igual". Se tiene un modelo del sistema axiomático.

b) Si A es el conjunto de las partes de un conjunto U, y $R$ es la relación de inclusión, entonces valen los axiomas y se tiene otro modelo del sistema.

### 7.2.2. Propiedades de los sistemas axiomáticos

No toda colección arbitraria de términos primitivos y de propiedades relativas a éstos caracteriza un sistema axiomático. Es necesario que de los axiomas no se derive ninguna contradicción, es decir, debe cumplirse la propiedad de compatibilidad o no contradicción. Si esto no ocurre, o sea, si en el desarrollo del sistema aparecen dos axiomas o teoremas contradictorios, entonces el sistema es incompatible o inconsisten-

te. La compatibilidad es eventualmente imposible de probar, ya que habría que agotar todos los teoremas de la teoría y comprobar su no contradicción. La compatibilidad de un sistema axiomático puede probarse indirectamente exhibiendo un modelo.

Otras propiedades son aconsejables en todo sistema axiomático, aunque no necesarias, Sin entrar en detalles, mencionamos las siguientes: independencia del sistema, en el sentido de que ningún axioma pueda probarse a expensas de los demás.

La no independencia de un axioma no niega la consistencia del sistema. Sea un axioma $A_i$ de un sistema compatible. Diremos que $A_i$ es independiente si y sólo si el sistema que se deduce del dado sustituyendo a $A_i$ por su negación, es compatible.

Si un sistema axiomático compatible es tal, que de sus axiomas se deduce la verdad o la falsedad de todo enunciado relativo a la teoría, entonces se dice que es completo o saturado.

Por otra parte, si dos modelos cualesquiera de un sistema son isomorfos respecto de las relaciones y operaciones definidas en los mismos, entonces se dice que dicho sistema es categórico. Se demuestra que la categoricidad de un sistema implica la saturación del mismo.

## 7.3. ALGEBRA DE BOOLE

### 7.3.1. Concepto

El sistema axiomático que conduce al álgebra de Boole consiste en

i ) *términos primitivos* son: un conjunto $B \neq \phi$ y dos funciones que se denotan con + y

ii ) *axiomas*

$B_1$ : + y . son dos leyes de composición interna en B.

$B_2$ : + y . son conmutativas.

$B_3$ : + y . son asociativas.

$B_4$ : + y . son distributivas, cada una respecto de la otra.

$B_5$ : Existen neutros en B, respecto de + y de que se denotan con 0 y 1, respectivamente.

$B_6$ : Todo elemento $a \in B$ admite un complementario $a'$, tal que

$$a + a' = 1 \quad \text{y} \quad a \,.\, a' = 0$$

*Ejemplo 7-2.*

Los siguientes son modelos del álgebra de Boole:

a) Si U es un conjunto, entonces el conjunto $P$ (U), de las partes de U, con la unión e intersección, constituye un modelo de álgebra de Boole, siendo el conjunto $\phi$ y el

mismo U los neutros para dichas operaciones. Además, todo subconjunto de U admite un complementario que satisface $B_6$.

b) Si $B = \{1, 2, 3, 5, 6, 10, 15, 30\} = \{x \in N \,/\, x \mid 30\}$, $+ = \vee$ denota el mínimo común múltiplo, y $. = \wedge$ significa el máximo común divisor, entonces resulta otro modelo de álgebra de Boole, donde los neutros son, respectivamente, 1 y 30.

### 7.3.2. Dualidad en el álgebra de Boole

Se llama proposición dual correspondiente a una proposición del álgebra de Boole, a la que se deduce de ella intercambiando los signos de las operaciones + y . , y sus elementos neutros 0 y 1.

Así, los duales de los seis axiomas relativos a la operación + son los seis correspondientes de la segunda operación.

El principio de dualidad establece que el dual de un teorema del álgebra de Boole es también un teorema del mismo sistema axiomático.

### 7.3.3. Propiedades del álgebra de Boole

Sea (B , + , .) un álgebra de Boole. Demostramos los siguientes teoremas:

I) Idempotencia

En efecto
$$a \in B \Rightarrow a\,.\,a = a$$

$$a \in B \Rightarrow a\,.\,1 = a \qquad \text{por } B_5$$
$$\Rightarrow a\,.\,(a + a') = a \qquad \text{por } B_6$$
$$\Rightarrow a\,.\,a + a\,.\,a' = a \qquad \text{por } B_4$$
$$\Rightarrow a\,.\,a + 0 = a \qquad \text{por } B_6$$
$$\Rightarrow a\,.\,a = a \qquad \text{por } B_5$$

Por el principio de dualidad se tiene

I') $a \in B \Rightarrow a + a = a$

II) $a + 1 = 1$

En efecto, por $B_6$, $B_3$, I' y $B_6$ tenemos

$$a + 1 = a + (a + a') = (a + a) + a' =$$
$$= a + a' = 1$$

Por dualidad resulta

II') $a\,.\,0 = 0$

III) Ley involutiva.

$$a \in B \Rightarrow (a')' = a$$

aplicando sucesivamente $B_5, B_6, B_2', B_4, B_2, B_6, B_6, B_4, B_6$ y $B_5$ resulta

$$\begin{aligned}(a')' &= (a')' + 0 = (a')' + (a \,.\, a') = \\ &= (a')' + (a' \,.\, a) = [(a')' + a'] \,.\, [(a')' + a] = \\ &= [a' + (a')'].[a + (a')'] = 1 \,.\, [a + (a')'] = \\ &= (a + a') \,.\, [a + (a')'] = a + [a' \,.\, (a')'] = \\ &= a + 0 = a\end{aligned}$$

IV) Ley de De Morgan

$$(a + b)' = a' \,.\, b'$$

Consideremos

$$\begin{aligned}(a + b) \,.\, (a' \,.\, b') &= (a' \,.\, b') \,.\, (a + b) = \\ &= [(a' \,.\, b') \,.\, a] + [(a' \,.\, b') \,.\, b] = \\ &= [(b' \,.\, a') \,.\, a] + [(a' \,.\, b') \,.\, b] = \\ &= [b' \,.\, (a' \,.\, a)] + [a' \,.\, (b' \,.\, b)] = \\ &= (b' \,.\, 0) + (a' \,.\, 0) = 0 + 0 = 0\end{aligned}$$

O sea

$$(a + b) \,.\, (a' \,.\, b') = 0 \qquad (1)$$

Análogamente, se llega a

$$(a + b) + (a' \,.\, b') = 1 \qquad (2)$$

De (1) y (2) resulta

$$(a + b)' = a' \,.\, b'$$

La forma dual es

IV') $(a \,.\, b)' = a' + b'$

## 7.4. SISTEMA AXIOMATICO DE PEANO

### 7.4.1. Teoría de Peano

El sistema axiomático de Peano es esencialmente ordinal, y define al conjunto de los números naturales algebrizado con las operaciones de adición y multiplicación, salvo isomorfismos. Consiste en

i ) *términos primitivos:*

un objeto, que se denota con 1

un conjunto $N \neq \phi$

una función, llamada "siguiente" o "sucesor", que se simboliza con "s".

ii ) *axiomas*

$A_1$ : el objeto 1 es un elemento de N, es decir

$$1 \in N$$

$A_2$ : la función "siguiente" es una aplicación inyectiva de N en $N - \{1\}$.

$$s : N \to N - \{1\} \quad \text{es} \quad 1\text{-}1$$

Este axioma establece

a) todo elemento de N tiene un sucesor y sólo uno.

b) el 1 no es sucesor de ningún elemento de N.

c) si dos elementos de N tienen el mismo sucesor, entonces son iguales.

$A_3$ : Principio de inducción completa. Si S es un subconjunto de N que contiene al 1, y al siguiente de $h$ siempre que contenga a $h$, entonces $S = N$. Es decir, si $S \subset N$ es tal que satisface

$$1 \in S$$

$$h \in S \Rightarrow s(h) \in S \quad , \quad \text{entonces} \quad S = N$$

Coincide con 6.4.2., y puede expresarse, de acuerdo con 6.4.3. de la siguiente manera: si P es una propiedad relativa a los elementos de N que satisface

i ) $P(1)$ es V

ii ) $P(h)$ es V $\Rightarrow P(s(h))$ es V, entonces $P(n)$ es V para todo $n \in N$.

iii) *definiciones*

I) *de adición*

a) $a + 1 = s(a)$ cualquiera que sea $a \in N$.

b) $a + s(b) = s(a + b)$ cualesquiera que sean $a$ y $b$ en N.

II) *de multiplicación*

a) $a \cdot 1 = a$ para todo $a \in N$.

b) $a \cdot s(b) = a \cdot b + a$ cualesquiera que sean $a$ y $b$ en N.

El sistema axiomático se completa con otras definiciones y teoremas, de los cuales demostraremos algunos a manera de ejemplos.

Interesa ver que las definiciones propuestas en I) y II) caracterizan leyes de composición interna en N. Lo verificamos en el caso de la adición, para lo cual hay que probar, de acuerdo con la definición de ley interna, que la suma de dos elementos cualesquiera de N es un único elemento de N, es decir

$$a \in N \ \wedge \ n \in N \Rightarrow a + n \quad \text{está unívocamente}$$

determinado en N, para todo $n \in N$.

En efecto, si S es el subconjunto de N formado por los elementos $n$ para los cuales existe y es único $a + n$, se tiene

i ) $n = 1 \Rightarrow a + 1 = s(a)$ por I a) y por $A_2$, está unívocamente determinado, es decir, $1 \in S$.

ii ) Hipótesis) $h \in S$.

Tesis) $s(h) \in S$.

Demostración)

$h \in S \Rightarrow a + h$ está unívocamente determinado por la definición de S.

Por $A_2$ y por la definición I b), $s(a + h) = a + s(h)$ está unívocamente determinado, y en consecuencia $s(h) \in S$.

Luego, $S = N$, y por consiguiente, la adición definida en I) es una ley de composición interna en N.

Con criterio análogo puede probarse que II) satisface la definición de ley de composición interna.

De acuerdo con lo demostrado, si denotamos

$2 = s(1)$ $3 = s(2)$, etc., para efectuar $3 + 2$, procedemos así:

$$3 + 2 = 3 + s(1) = s(3 + 1) = s(s(3)) = s(4) = 5$$

teniendo en cuenta la definición de 2, I b), I a), la definición de 4, y la definición de 5.

*Ejemplo 7-3.*

Si consideramos las sucesiones

$$10, 11, 12, 13, \ldots\ldots$$
$$1, 1/3, 1/9, 1/27, \ldots$$

vemos que satisfacen los axiomas de Peano, pero si los algebrizamos de acuerdo con su teoría, se tiene

$$11 + 10 = 12$$
$$1/3 + 1 = 1/9$$

siendo estos resultados distintos de los de la aritmética ordinaria. Se tienen, así, dos modelos del sistema axiomático, los cuales son isomorfos a $N = \{1, 2, 3, \ldots\}$. En última instancia son dos representaciones distintas de N.

### 7.4.2. Propiedades

Demostramos los siguientes teoremas de la teoría de Peano.

1. *La función sucesor es sobreyectiva.* En otras palabras, todo número natural distinto de 1 es el siguiente de otro.

Hay que probar que la imagen de la función sucesor es el conjunto $\mathbf{N} - \{1\}$
Sea S el conjunto de las imágenes de los elementos de N.

i) $2 = s(1)$ pertenece a S.

ii) Si $h \in S$, entonces $s(h) \in S$. En efecto:

$$h \in S \Rightarrow h \in \mathbf{N} \Rightarrow s(h) \in S$$

2. *La adición es asociativa en* N

$$(a + b) + n = a + (b + n).$$

Demostración)

i) $n = 1 \Rightarrow (a + b) + 1 = s(a + b) =$
$= a + s(b) = a + (b + 1)$

Por I b) y I a)

ii) $(a + b) + h = a + (b + h) \Rightarrow (a + b) + s(h) = a + [b + s(h)]$

En efecto

$$\begin{aligned}(a + b) + s(h) &= s[(a + b) + h] = \\ &= s[a + (b + h)] = a + s(b + h) = \\ &= a + [b + s(h)]\end{aligned}$$

Por I b), hipótesis y I b).

3. *La adición es conmutativa en* N.
Lo demostramos en dos situaciones:

I) $n + 1 = 1 + n$

i) $n = 1 \Rightarrow 1 + 1 = 1 + 1$

ii) $h + 1 = 1 + h \Rightarrow s(h) + 1 = 1 + s(h)$

En efecto

$$\begin{aligned}1 + s(h) &= 1 + (h + 1) = (1 + h) + 1 = \\ &= s(h) + 1\end{aligned}$$

Aplicando la definición I a), la asociatividad y I a).

II) $a + n = n + a$

i) $n = 1 \Rightarrow a + 1 = 1 + a$ por I)

ii) $a + h = h + a \Rightarrow a + s(h) = s(h) + a$

Demostración)

$$\begin{aligned}a + s(h) &= a + (h + 1) = (a + h) + 1 = \\ &= (h + a) + 1 = h + (a + 1) = \\ &= h + (1 + a) = (h + 1) + a = s(h) + a\end{aligned}$$

En virtud de I a), asociatividad, hipótesis, asociatividad, i ), asociatividad y I a).

4. *El 1 es neutro para la multiplicación, es decir,* $n \,.\, 1 = 1 \,.\, n = n$.

En efecto.

i ) $n = 1 \Rightarrow 1 \,.\, 1 = 1 \,.\, 1 = 1$

ii ) $h \,.\, 1 = 1 \,.\, h \Rightarrow s(h) \,.\, 1 = 1 \,.\, s(h)$

Sea

$$s(h) \,.\, 1 = s(h) = h + 1 =$$
$$= h \,.\, 1 + 1 = 1 \,.\, h + 1 =$$
$$= 1 \,.\, s(h)$$

Se han utilizado II a), la hipótesis y II b).

5. *La multiplicación es distributiva respecto de la adición.*

Se trata de probar que cualquiera que sea $n \in \mathbf{N}$

$$(a + b) \,.\, n = a \,.\, n + b \,.\, n$$

i ) $n = 1 \Rightarrow (a + b) \,.\, 1 = a + b = a \,.\, 1 + b \,.\, 1$

por II a)

ii ) $(a + b) \,.\, h = a \,.\, h + b \,.\, h \Rightarrow (a + b)\, s(h) = a \,.\, s(h) + b \,.\, s(h)$

En efecto

$$(a + b) \,.\, s(h) = (a + b) \,.\, h + (a + b) =$$
$$= (a \,.\, h + b \,.\, h) + (a + b) = (a \,.\, h + a) + (b \,.\, h + b) =$$
$$= a \,.\, s(h) + b \,.\, s(h)$$

donde hemos aplicado II b), la hipótesis, conmutatividad y asociatividad de la adición, y II b).

6. *La multiplicackón es asociativa.*

$$(a \,.\, b) \,.\, n = a \,.\, (b \,.\, n)$$

i ) $n = 1 \Rightarrow (a \,.\, b) \,.\, 1 = a \,.\, b = a \,.\, (b \,.\, 1)$

de acuerdo con II a).

ii ) $(a \,.\, b) \,.\, h = a \,.\, (b \,.\, h) \Rightarrow (a \,.\, b) \,.\, s(h) = a \,.\, [b \,.\, s(h)]$

Sea

$$(a \,.\, b) \,.\, s(h) = (a \,.\, b) \,.\, h + (a \,.\, b) =$$
$$= a \,.\, (b \,.\, h) + a \,.\, b = a \,.\, (b \,.\, h + b) =$$
$$= a \,.\, [b \,.\, s(h)]$$

por aplicación de II b), la hipótesis, distributividad y II b).

### 7.4.3. Otra forma equivalente de la teoría de Peano

En el conjunto **N** no figura como elemento el 0. Peano mismo lo introdujo en otra versión de su sistema axiomático, y muchos autores prefieren incluirlo. En este caso no se modifican los axiomas esencialmente, salvo que el 1 se sustituye por el símbolo 0. Sin embargo, hay que cambiar las definiciones de adición y multiplicación, las cuales adoptan las siguientes expresiones:

I) Adición

a) $a + 0 = a$

b) $a + s(b) = s(a + b)$

II) Multiplicación

a) $a \, . \, 0 = 0$

b) $a \, . \, s(b) = a \, . \, b + a$

En este caso se define $1 = s(0)$.

*Ejemplo 7-4.*

Demostrar

$$a \, . \, n = \underbrace{a + a + \ldots + a}_{n} = \sum_{i=1}^{n} a$$

Hacemos inducción sobre $n$.

i ) $n = 1 \Rightarrow a \, . \, 1 = a = \sum\limits_{i=1}^{1} a$

ii ) Hipótesis) $\quad a \, . \, h = \sum\limits_{i=1}^{h} a$

Tesis) $\quad a \, . \, (h + 1) = \sum\limits_{i=1}^{h+1} a$

Demostración)

Por definición II b)

$$a \, . \, (h + 1) = a \, . \, h + a$$

Por hipótesis

$$a \, . \, (h + 1) = \sum_{i=1}^{h} a + a$$

Por propiedad de la sumatoria

$$a \, . \, (h + 1) = \sum_{i=1}^{h+1} a$$

De este modo queda demostrada la expresión habitual de producto de un número natural $a$, por $n \in \mathbf{N}$, que se da como definición en la escuela secundaria.

*Ejemplo 7-5.*

Se define la potenciación en **N**, mediante

a) $a^1 = a$

b) $a^{s(b)} = a^b \cdot a$

Demostramos las siguientes propiedades por inducción completa.

I) *Distributividad respecto del producto.*

$$(a \cdot b)^n = a^n \cdot b^n$$

i ) $n = 1 \Rightarrow (a \cdot b)^1 = a \cdot b = a^1 \cdot b^1$

por la definición a)

ii ) $(a \cdot b)^h = a^h \cdot b^h \Rightarrow (a \cdot b)^{s(h)} = a^{s(h)} \cdot b^{s(h)}$

Por definición b), hipótesis inductiva, conmutatividad y asociatividad del producto, y nuevamente por definición b), resulta:

$$(a \cdot b)^{s(h)} = (a \cdot b)^h \cdot (a \cdot b) = a^h \cdot b^h \cdot a \cdot b =$$
$$= a^h \cdot a \cdot b^h \cdot b = a^{s(h)} \cdot b^{s(h)}$$

II) *Regla del producto de potencias de igual base*

$$a^m \cdot a^n = a^{m+n}$$

Hacemos inducción sobre $n$

i ) $n = 1 \Rightarrow a^m \cdot a^1 = a^m \cdot a = a^{s(m)} = a^{m+1}$

por las definiciones a) y b).

ii ) $a^m \cdot a^h = a^{m+h} \Rightarrow a^m \cdot a^{s(h)} = a^{m+s(h)}$

En efecto, si aplicamos sucesivamente la definición b), asociatividad del producto, la hipótesis y las definiciones b) de potenciación y adición, resulta

$$a^m \cdot a^{s(h)} = a^m\,(a^h \cdot a) = (a^m \cdot a^h) \cdot a =$$
$$= a^{m+h} \cdot a = a^{s(m+h)} = a^{m+s(h)}$$

*Ejemplo 7-6.*

En **N** se define la relación de menor, mediante

$$a < b \Leftrightarrow \exists\, x \in \mathbf{N} \,/\, b = a + x \qquad (1)$$

Demostramos las siguientes propiedades:

I) Todo número natural es menor que su sucesor, es decir

$$n < s(n)$$

i) $n = 1 \Rightarrow s(1) = 1 + 1 \Rightarrow 1 < s(1)$

por las definiciones a) de adición, y (1).

ii) $h < s(h) \Rightarrow h + 1 < s(h + 1)$

En efecto

$$s(h+1) = s(1+h) = 1 + s(h) =$$
$$= 1 + (h+1) = (h+1) + 1$$

Entonces, por (1)

$$h + 1 < s(h+1)$$

III) La relación de menor es transitiva

$$a < b \quad \text{y} \quad b < c \Rightarrow a < c$$

En efecto, por (1)

$$a < b \quad \text{y} \quad b < c \Rightarrow$$
$$\Rightarrow \exists\, x\,,\, y \in \mathbf{N} \,/\, b = a + x \ \wedge \ c = b + y \Rightarrow$$
$$\Rightarrow c = (a + x) + y \Rightarrow c = a + (x + y) \Rightarrow$$
$$\Rightarrow a < c$$

IV) Leyes de monotonía

a) $a < b \Rightarrow a + c < b + c$

b) $a < b \ \wedge \ c < d \Rightarrow a + c < b + d$

Demostramos a)

$$a < b \Rightarrow \exists\, x \in \mathbf{N} \,/\, b = a + x \Rightarrow$$
$$\Rightarrow b + c = (a + x) + c \Rightarrow$$
$$\Rightarrow b + c = (a + c) + x \Rightarrow b + c < a + c$$

La parte b) queda como ejercicio.

## 7.5. ESTRUCTURA DE MONOIDE

### 7.5.1. Concepto de estructura algebraica

En su forma más simple, una estructura algebraica es un objeto matemático consistente en un conjunto no vacío y una relación o ley de composición interna definidas en él. En situaciones más complicadas puede definirse más de una ley de composición interna en el conjunto, y también leyes de composición externas. Según sean las propiedades que deban satisfacer dichas leyes de composición, se tienen los distintos tipos de estructuras algebraicas, que son, exactamente, sistemas axiomáticos.

### 7.5.2. Estructura de monoide

No existe un criterio uniforme en cuanto a la definición de monoide. Claude Chevalley, en *Fundamental Concepts of Algebra*, lo introduce como un conjunto dotado de una ley de composición interna, asociativa y con elemento neutro. Adoptamos la definición que expone Enzo R. Gentile, en *Estructuras algebraicas*, monografía N° 3 de la O.E.A., en la que se exigen menos condiciones.

***Definición***

El par $(M\ ,\ *)$, donde $M \neq \phi$, y $*$ es una función, es un monoide si y sólo si $*$ es una ley de composición interna en M.

En este sistema axiomático los términos primitivos son M y $*$, y el único axioma establece que $*$ es una función de $M^2$ en M.

Son modelos de monoides los conjuntos **N**, **Z**, **Q**, **R** y **C**, con la adición ordinaria de números.

En cambio, el par $(\mathbf{N}, -)$ no es un monoide, ya que la sustracción no es ley de composición interna en **N**.

El par $(\mathbf{N}, *)$, donde $*$ está definida mediante

$$a * b = \text{máx}\left\{a\ ,\ b\right\} \qquad \text{tiene estructura de monoide.}$$

## 7.6. ESTRUCTURA DE SEMIGRUPO

***Definición***

El par $(A, *)$, donde $A \neq \phi$ y $*$ es una función, es un semigrupo si y sólo si $*$ es ley interna y asociativa en A.

En otras palabras, un semigrupo es un monoide asociativo.

En particular, si la ley de composición es conmutativa, entonces el semigrupo se llama conmutativo; y si existe elemento neutro, se dice que el semigrupo tiene unidad. El elemento neutro suele llamarse identidad.

El par $(\mathbf{N}\ ,\ +)$ es un semigrupo conmutativo, sin neutro. En cambio $(\mathbf{N_0}\ ,\ +)$ tiene elemento neutro 0.

El objeto $(\mathbf{N}\ ,\ .)$ es un semigrupo conmutativo, con elemento neutro o identidad igual a 1.

*Ejemplo 7-7.*

Sea $(M\ ,\ *)$ un monoide. Se definen los elementos identidad (o neutro) a izquierda o derecha, mediante

i ) $e \in M$ es identidad a izquierda $\Leftrightarrow \forall a : a \in M \Rightarrow e * a = a$

ii ) $e \in M$ es identidad a derecha $\Leftrightarrow \forall a : a \in M \Rightarrow a * e = a$

Es claro que los elementos de identidad, si existen, lo son respecto de $*$.

Demostrar que si $e'$ y $e''$ son identidades a izquierda y a derecha del monoide, entonces $e' = e''$.

$$e'' = e' * e'' = e'$$

Por ser $e'$ neutro a izquierda, y $e''$ neutro a derecha.

Si un monoide tiene identidad a izquierda y a derecha, se dice que tiene identidad.

El monoide $(\mathbf{Z}, -)$ tiene sólo identidad a derecha, y es 0, pues

$$\forall x : x \in \mathbf{Z} \Rightarrow x - 0 = x$$

***Ejemplo 7-8.***

Sean $A \neq \phi$, y $A^A$ el conjunto de todas las funciones de A en A, es decir

$$A^A = \left\{ f / f : A \to A \right\}$$

Entonces, si "$\circ$" denota la composición de funciones, el par $(A^A, \circ)$ es un semigrupo con elemento neutro o identidad. En efecto

$$A_1 : f \in A^A \ \wedge \ g \in A^A \Rightarrow f : A \to A \ \wedge \ g : A \to A \Rightarrow g \circ f : A \to A$$

Es decir, la composición es ley interna en $A^A$.

$A_2$ : asociatividad

$$f, g, h \in A^A \Rightarrow (h \circ g) \circ f = h \circ (g \circ f)$$

ya que la composición de funciones es asociativa.

$A_3$ : Neutro es $i_A \in A^A$, ya que

$$i_A \circ f = f \circ i_A = f \qquad \text{cualquiera que sea} \qquad f \in A^A$$

***Ejemplo 7-9.***

Sea $(M, *)$ un monoide con neutro o identidad $e \in M$.

Por definición

i ) $a_1 \in M$ es inverso a izquierda de $a \in M$, respecto de $*$, si y sólo si

$$a_1 * a = e$$

ii ) $a_2 \in M$ es inverso a derecha de $a \in M$, respecto de $*$, si y sólo si

$$a * a_2 = e$$

iii) $a'$ es inverso de $a$ respecto de $*$, si y sólo si lo es a izquierda y a derecha, es decir

$$a' * a = a * a' = e$$

En este caso, se dice que $a \in M$ es un elemento inversible del monoide.
Sea el monoide definido por la siguiente tabla:

| * | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ | $c$ | $d$ |
| $c$ | $b$ | $c$ | $d$ | $c$ |
| $d$ | $c$ | $d$ | $b$ | $b$ |

De la observación de la tabla surge que el neutro es $b$.

Determinamos los inversos:

| elementos | inversos a izquierda | a derecha | inversos |
|---|---|---|---|
| $a$ | $c$ | – | — |
| $b$ | $b$ | $b$ | $b$ |
| $c$ | $d$ | $a$ | – |
| $d$ | $d$ | $c$ | $d$ |

## TRABAJO PRACTICO VII

*7-10.* Sea un sistema axiomático compatible, con los axiomas $A_1, A_2, \ldots, A_n$. Por definición, el axioma $A_i$ es independiente si y sólo si el sistema cuyos axiomas son $A_1, A_2, \ldots, A_{i-1}, \sim A_i, \ldots, A_n$, es compatible.
Demostrar la independencia de los tres axiomas del ejemplo 7-1.

*7-11.* Se considera el siguiente sistema axiomático

i ) términos primitivos: $A \neq \phi$ y $R \subset A^2$

ii ) axiomas

$$A_1 : a \neq b \Rightarrow (a, b) \in R \;\vee\; (b, a) \in R$$
$$A_2 : (a, b) \in R \Rightarrow a \neq b$$
$$A_3 : (a, b) \in R \;\wedge\; (b, c) \in R \Rightarrow (a, c) \in R$$
$$A_4 : c(A) = 4$$

Demostrar

I. $(a, b) \in R \Rightarrow (b, a) \notin R$

II. $x \neq a \;\wedge\; x \neq b \;\wedge\; (a, b) \in R \Rightarrow (a, x) \in R \veebar (x, b) \in R$

*7-12.* Sea $(B, +, .)$ un álgebra de Boole. Demostrar

I. $1' = 0 \;\wedge\; 0' = 1$

II. El complementario de $a \in B$, es único.

III. $a + (a.b) = a \;\wedge\; a.(a + b) = a$

*7-13.* Demostrar que en N no existe neutro para la adición, es decir

$$a \in \mathbf{N} \;\wedge\; b \in \mathbf{N} \Rightarrow a + b \neq a$$

*7-14.* Demostrar en N

$$a \neq b \Rightarrow a + n \neq b + n$$

*7-15.* Demostrar que la multiplicación es conmutativa en N en las siguientes etapas:

i ) $n.1 = 1.n$

ii ) $s(b).n = b.n + n$

iii) $a.n = n.a$

**7-16.** Demostrar en N

i ) $a < b \Rightarrow a \cdot c < b \cdot c$

ii ) $a < b \wedge c < d \Rightarrow a \cdot c < b \cdot d$

iii) $a \cdot b = 1 \Rightarrow a = 1 \wedge b = 1$

**7-17.** Verificar si (M , *) es un monoide en los siguientes casos

i ) $M = N$

$a * b = a - b$

ii ) $M = Z$

$a * b = a - b$

iii) $M = R^{2 \times 2}$

$A * B = A - 2 \cdot B$

**7-18.** Demostrar que en todo semigrupo se verifica

i ) $(a * b) * c * d = a * (b * c) * d = a * b * (c * d)$

ii ) $a^m * a^n = a^{m+n}$

siendo $a^m = \underbrace{a * a * \ldots * a}_{m}$ y $m \in N$ y $n \in N$

**7-19.** Sean (A , *) un semigrupo y $\phi \neq S \subset A$. Por definición (S , *) es un sub-semigrupo de (A , *) si y sólo si (S , *) es un semigrupo.
Demostrar que la intersección de toda familia de sub-semigrupos de A, es un sub-semigrupo de A.

**7-20.** Sean (A , *) un semigrupo y S una parte no vacía de A. La intersección de todos los sub-semigrupos que contienen a S se llama sub-semigrupo generado por S, y lo denotamos por

$$\overline{S} = \bigcap_{S_i \supset S} S_i$$

donde cada $S_i$ es un sub-semigrupo que contiene a S.
Si $\overline{S} = A$, entonces se dice que A está generado por S.
Verificar, para (N , +) y (Z , +)

i ) $S = \{1\} \Rightarrow \overline{S} = N$

ii) $S = \{1, -1\} \Rightarrow \overline{S} = Z$

Capítulo 8

# ESTRUCTURA DE GRUPO

## 8.1. INTRODUCCION

La estructura de grupo es un sistema axiomático básico y fundamental de la matemática y puede ser encarada imponiendo condiciones a las estructuras de monoide o de semigrupo, introducidas en el capítulo anterior. No obstante, como es habitual, la proponemos aquí independientemente de aquellos conceptos, los cuales suelen obviarse en los cursos básicos. Después de encarar las propiedades generales y exponer ejemplos, se estudian los subgrupos, grupos finitos, grupos cíclicos, los homomorfismos de grupos y el concepto de grupo cociente.

## 8.2. EL CONCEPTO DE GRUPO

### 8.2.1. Definición de grupo

Sean un conjunto no vacío G, y una función $*$. El par $(G, *)$ es un grupo si y sólo si $*$ es una ley interna en G, asociativa, con neutro, y tal que todo elemento de G admite inverso respecto de $*$.

En forma simbólica, se tiene

***Definición***

$(G, *)$ es un grupo si y sólo si se verifican los axiomas

$G_1$ . $* : G^2 \to G$

$G_2$ . Asociatividad

$$\forall a \,\forall b \,\forall c : a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$$

$G_3$ . Existencia de elemento neutro o identidad

$$\exists e \in G \,/\, \forall a : a \in G \Rightarrow a * e = e * a = a$$

$G_4$ . Existencia de inversos

$$\forall a \in G, \exists a' \in G / a * a' = a' * a = e$$

Si además se verifica

$G_5$ . Conmutatividad

$$\forall a \forall b : a, b \in G \Rightarrow a * b = b * a$$

entonces el grupo se llama conmutativo o abeliano.

***Ejemplo 8-1.***

En el conjunto **Z** de los enteros se define $*$ mediante

$$a * b = a + b + 3 \qquad (1)$$

El par $(\mathbf{Z}, *)$ es un grupo abeliano. En efecto, se verifican:

$G_1$ . $*$ es ley interna en **Z**, por (1)

$G_2$ . $*$ es asociativa, pues

$$(a * b) * c = (a + b + 3) * c = a + b + 3 + c + 3 =$$
$$= a + b + c + 6 \qquad (2)$$
$$a * (b * c) = a * (b + c + 3) = a + b + c + 3 + 3 =$$
$$= a + b + c + 6 \qquad (3)$$

De (2) y (3) resulta

$$(a * b) * c = a * (b * c)$$

$G_3$ . Existe neutro en **Z** respecto de $*$

Si $e$ es neutro, entonces $a * e = a$.

Por (1) $a + e + 3 = a$ y resulta $e = -3$.

Análogamente se prueba que $-3$ es neutro a izquierda.

$G_4$ . Todo elemento de G es inversible respecto de $*$

Si $a'$ es inverso de $a$, entonces debe verificarse

$$a * a' = e$$

Teniendo en cuenta (1) y que $e = -3$

$$a + a' + 3 = -3$$

Luego

$$a' = -6 - a$$

De modo análogo se prueba que es inverso a izquierda.

$G_5$ . $*$ es conmutativa, ya que

$$a * b = a + b + 3 = b + a + 3 = b * a$$

de acuerdo con (1) y con la conmutatividad de la suma ordinaria en **Z**.

***Ejemplo 8-2.***

i ) Las siguientes interpretaciones constituyen modelos de grupos abelianos:

$$(\mathbf{Z}, +), (\mathbf{Q}, +), (\mathbf{R}, +), (\mathbf{C}, +)$$

como la operación es la suma, se llaman grupos aditivos.

ii ) En cambio no son modelos las interpretaciones

$(\mathbf{N}, +)$ pues no existen neutro en **N**, ni inverso de cada elemento.

$(\mathbf{N}_0, +)$ ya que si bien existe neutro 0, los demás elementos carecen de inverso aditivo.

$(\mathbf{Q}, .)$ no verifica $G_4$, porque 0 carece de inverso multiplicativo.

$(\mathbf{R}, .)$ por la misma razón.

iii) Son grupos

$$(\mathbf{Q}-\{0\}, .) \quad \text{y} \quad (\mathbf{R}-\{0\}, .)$$

***Ejemplo 8-3.***

Sean $A \neq \phi$, y $T(A)$ el conjunto de todas las funciones biyectivas de A en A, es decir

$$T(A) = \{f: A \to A \,/\, f \text{ es biyectiva}\}$$

Entonces $(T(A), \circ)$ es un grupo, donde "$\circ$" es la composición de aplicaciones.

En efecto

$G_1$ . La composición de aplicaciones es ley interna en T (A), pues

$$f \wedge g \in T(A) \Rightarrow g \circ f \in T(A)$$

ya que la composición de aplicaciones biyectivas de A en A es una función biyectiva de A en A, según 4.6.5.

$G_2$ . La composición de funciones en T (A) es asociativa

$$h, g, f \in T(A) \Rightarrow h \circ (g \circ f) = (h \circ g) \circ f$$

por lo demostrado en 4.6.2.

$G_3$ . La función $i_A \in T(A)$ es neutro para la composición.

La función identidad en A, definida en 4.5.2. mediante

$$i_A(x) = x \quad \text{para todo} \quad x \in A,$$

es neutro a izquierda y a derecha, ya que es biyectiva de A en A, es decir, es un elemento de T (A), y satisface

$$f \circ i_A = i_A \circ f = f \quad \text{cualquiera que sea} \quad f \in T(A)$$

como es fácil verificar usando la definición de composición y de funciones iguales.

$G_4$ . Todo elemento de T (A) admite inverso respecto de la composición.

Si $f \in$ T (A), entonces es una función biyectiva de A en A, y admite inversa $f^{-1}$, por 4.7.2. II, la cual es también biyectiva de A en A, es decir, un elemento de T (A).

El grupo (T (A) , ∘) se llama grupo de las transformaciones de A.

### 8.2.2. Cuestiones de notación

Sea (G , ∗) un grupo.

i ) Si la ley de composición es aditiva, suele denotarse con el signo +, y si $a \in G$, entonces su inverso aditivo suele llamarse opuesto y se indica $a' = -a$.

ii) Si la ley ∗ es multiplicativa se la indica con ".", el inverso multiplicativo de cada elemento $a$ se escribe $a' = a^{-1}$ y se dice que es el recíproco de $a$.

iii) En ocasiones, al referirnos al grupo (G , ∗), cometiendo un abuso de lenguaje, diremos el grupo G, sobreentendiendo la referencia a la ley de composición interna.

## 8.3. PROPIEDADES DE LOS GRUPOS

### 8.3.1. Unicidad del neutro y del inverso

De acuerdo con lo demostrado en 5.3.5. y 5.3.6., el elemento neutro es único y el inverso de cada elemento es único.

### 8.3.2. Regularidad

Los elementos de todo grupo son regulares.

Hipótesis) (G , ∗) es grupo

$$a * b = a * c$$

$$b * a = c * a$$

Tesis) $b = c$

Demostración)

Por hipótesis

$$a * b = a * c$$

Componiendo a izquierda con $a'$, inverso de $a$

$$a' * (a * b) = a' * (a * c)$$

Por asociatividad

$$(a' * a) * b = (a' * a) * c$$

Por $G_4$

$$e * b = e * c$$

Por $G_3$

$$b = c$$

Análogamente se prueba la regularidad a derecha.

La regularidad significa que la ley cancelativa es válida para todos los elementos del grupo.

### 8.3.3. Ecuaciones en un grupo

Sea $(G , *)$ un grupo. Entonces, cada una de las ecuaciones $b * x = a$ y $x * b = a$ admite solución única.

Componiendo los dos miembros de la primera ecuación a izquierda con $b'$, se tiene

$$b' * (b * x) = b' * a$$

Por $G_2$

$$(b' * b) * x = b' * a$$

Por $G_4$

$$e * x = b' * a$$

Por $G_3$

$$x = b' * a$$

La unicidad de la solución se debe a la unicidad del inverso, y al hecho de que $*$ es una función de $G^2$ en G.

El trabajo es análogo considerando la segunda ecuación.

En particular, se presentan estos casos:

i ) Si el grupo es aditivo, la ecuación $x * b = a$ se traduce en

$$x + b = a$$

y la solución hallada, es $x = a + (-b)$, donde $-b$ es el inverso de $b$.

Por definición, la suma de un elemento con el opuesto de otro se llama diferencia entre los mismos, y se escribe

$$x = a - b$$

Vinculando este resultado con la ecuación propuesta, queda justificada la trasposición de términos de un miembro a otro de una igualdad.

ii ) Supongamos un grupo multiplicativo, y la segunda ecuación, que se convierte en

$$x \, . \, b = a$$

Al componer a derecha con el inverso multiplicativo de $b$, resulta la solución

$$x = a \,.\, b^{-1}$$

Por definición, el producto de un elemento del grupo por el inverso multiplicativo de otro se llama cociente y se expresa

$$x = \frac{a}{b}$$

Entonces, en los grupos multiplicativos numéricos es lícito el pasaje de factores no nulos de un miembro al otro, como divisores.

### 8.3.4. Inverso de la composición

En todo grupo, el inverso de la composición de dos elementos es igual a la composición de los inversos en orden permutado.

Se trata de probar que

$$(a * b)' = b' * a'$$

Antes de entrar en el detalle de la demostración, proponemos dos resultados útiles

i ) Cualquiera de las ecuaciones $a * x = a$ ó $x * a = a$ admite la solución $x = e$.

Si consideramos la primera, después de componer a izquierda con $a'$, se llega a $x = e$, y análogamente en el segundo caso componiendo a derecha con el mismo $a'$.

ii) Cualquiera de las ecuaciones $a * x = e$ ó $x * a = e$ admite la solución $x = a'$.

Sea $a * x = e$; luego de componer a izquierda con $a'$, se tiene $x = a'$. El mismo resultado se obtiene a partir de la segunda ecuación, después de componer a derecha con $a'$.

iii) Demostramos ahora la proposición inicial.

Hipótesis) $(G , *)$ es grupo

Tesis) $(a * b)' = b' * a'$

Demostración)

Una traducción de la propiedad ii ) es la siguiente: si la composición de dos elementos es el neutro, entonces cada uno es el inverso del otro.

Sea entonces

$$(a * b) * (b' * a')$$

Aplicando sucesivamente $G_2, G_4, G_3$ y $G_4$, resulta

$$(a * b) * (b' * a') = a * (b * b') * a' * e * a = a' * a = e$$

y por ii ), se tiene

$$(a * b)' = b' * a'$$

Y también

$$(b' * a')' = a * b$$

## 8.4. SUBGRUPOS

### 8.4.1. Definición

El subconjunto no vacío H, del grupo G, es un subgrupo de $(G , *)$ si y sólo si $(H , *)$ es grupo.

*Ejemplo 8-4.*

i ) Todo grupo $(G , *)$ admite como subgrupos al mismo G, y al conjunto cuyo único elemento es $e$. Ambos se llaman subgrupos triviales de $(G , *)$.

ii ) $(\mathbf{Z} , +)$ es subgrupo de $(\mathbf{Q} , +)$.

iii) El conjunto de los enteros pares, con la adición, es un subgrupo de $(\mathbf{Z} , +)$. En cambio no lo es el conjunto de los enteros impares con la misma ley, ya que la suma de dos enteros impares es par y no se verifica $G_1$.

iv) El grupo de los cuatro elementos de Klein consiste en el conjunto $A = \{a , b , c , d\}$, con la ley de composición definida por la tabla

| $*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $a$ | $d$ | $c$ |
| $c$ | $c$ | $d$ | $a$ | $b$ |
| $d$ | $d$ | $c$ | $b$ | $a$ |

Su construcción es simple, observando las diagonales y la simetría que se presenta respecto de ellas.

Es fácil verificar que el grupo es abeliano, y que cada elemento se identifica con su inverso, siendo el neutro $a$.

Un subgrupo de $(A , *)$ es $H = \{a , b\}$.

En cambio, no lo es el subconjunto $H' = \{a , b , c\}$ ya que $b * c = d \notin H'$.

### 8.4.2. Condición suficiente para la existencia de subgrupo

En el ejemplo 8-4 se ha verificado que no toda parte no vacía de un grupo es un subgrupo. Además de ser una parte no vacía, la definición exige que tenga estructura de grupo con la misma ley de composición. Ahora, bien, esto obliga a la investigación de los cuatro axiomas, y resulta conveniente disponer de alguna condición más económica, que permita decidir si se trata de un subgrupo.

***Teorema***

Si H es un subconjunto no vacío del grupo (G , $*$), que verifica

$$a \in H \wedge b \in H \Rightarrow a * b' \in H$$

entonces (H , $*$) es un subgrupo de (G , $*$).

Hipótesis) (G , $*$) es grupo

$\phi \neq H \subset G$

$a \in H \wedge b \in H \Rightarrow a * b' \in H$

Tesis) (H , $*$) es subgrupo de (G , $*$)

Demostración)

Debemos probar que se cumplen los axiomas de grupo para H.

I) La asociatividad de $*$ en H se verifica por ser $H \subset G$.

II) El neutro pertenece a H. En efecto

$$H \neq \phi \Rightarrow \exists\, a \in H$$

Por hipótesis y definición de inverso

$$a \in H \wedge a \in H \Rightarrow a * a' \in H \Rightarrow e \in H$$

III) Todo elemento de H admite su inverso en H.

Sea $a \in H$.

Por II y por hipótesis

$$e \in H \wedge a \in H \Rightarrow e * a' \in H \Rightarrow a' \in H$$

IV) H es cerrado para la ley $*$.

Sean $a \in H \wedge b \in H$.

Por III, por hipótesis y por inverso del inverso, se tiene

$$a \in H \wedge b \in H \Rightarrow a \in H \wedge b' \in H \Rightarrow a * (b')' \in H \Rightarrow$$
$$\Rightarrow a * b \in H$$

Lo demostrado en I, II, III, IV prueba que (H , $*$) es un subgrupo de (G , $*$). Esta condición suficiente es obviamente necesaria. Se la utiliza en la práctica de la siguiente manera: de acuerdo con la hipótesis del teorema, para que H sea un subgrupo de (G , $*$) debemos probar

i ) $H \neq \phi$

ii ) $H \subset G$

iii) Si dos elementos cualesquiera pertenecen a H, entonces el primero, compuesto con el inverso del segundo, debe pertenecer a H.

***Ejemplo 8-5.***

En $\mathbf{R}^2$ definimos la suma de pares ordenados de números reales

$$(a , b) + (c , d) = (a + c , b + d) \qquad (1)$$

Comprobamos que $(\mathbf{R}^2, +)$ tiene estructura de grupo abeliano, ya que se verifican:
$G_1$. La suma de pares definida en (1) es ley de composición interna en $\mathbf{R}^2$.
$G_2$. Asociatividad.

$$[(a, b) + (c, d)] + (e, f) = (a + c, b + d) + (e, f) =$$
$$= ((a + c) + e, (b + d) + f) = (a + (c + e), b + (d + f)) =$$
$$= (a, b) + (c + e, d + f) = (a, b) + [(c, d) + (e, f)$$

Por (1), asociatividad de la suma en $\mathbf{R}$ y (1).
$G_3$. Neutro es el par $(0, 0)$, ya que

$$(a, b) + (0, 0) = (0, 0) + (a, b) = (a, b)$$

$G_4$. Inverso aditivo u opuesto del par $(a, b)$, es el par $(-a, -b)$, pues

$$(a, b) + (-a, -b) = (-a, -b) + (a, b) = (0, 0)$$

$G_5$. Conmutatividad.

$$(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) =$$
$$= (c, d) + (a, b)$$

Por (1), conmutatividad de la suma en $\mathbf{R}$, y (1).
$(\mathbf{R}^2, +)$ es el grupo abeliano de los pares ordenados de números reales con la suma ordinaria de pares.

***Ejemplo 8-6.***

Sean el grupo $(\mathbf{R}^2, +)$, y

$$\mathrm{H} = \left\{(x, y) \in \mathbf{R}^2 \ / \ y = 2x\right\}$$

Es claro que un elemento de $\mathbf{R}^2$ pertenece a H si y sólo si la segunda componente es el duplo de la primera.
Comprobaremos que $(\mathrm{H}, +)$ es un subgrupo de $(\mathbf{R}^2, +)$.
Verificamos las hipótesis de la condición suficiente demostrada

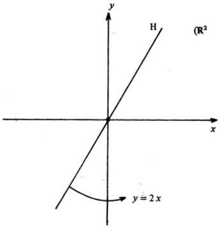
i ) $\mathrm{H} \neq \phi$, ya que $(1, 2) \in \mathrm{H}$.
ii ) $\mathrm{H} \subset \mathrm{G}$ por la definición de H.
iii) Sean $(a, b) \in \mathrm{H}$ y $(c, d) \in \mathrm{H}$; debemos probar que $(a, b) + (-c, -d) \in \mathrm{H}$.
En efecto:

$$(a, b) \in \mathrm{H} \ \wedge \ (c, d) \in \mathrm{H} \Rightarrow b = 2a \ \wedge \ d = 2c \Rightarrow b - d = 2(a - c) \Rightarrow$$
$$\Rightarrow (a - c, b - d) \in \mathrm{H} \Rightarrow (a, b) + (-c, -d) \in \mathrm{H}$$

Hemos utilizado la definición de H, la sustracción en $\mathbf{R}$, la definición de H, y la de suma de pares.

Gráficamente, H consiste en la recta que pasa por el origen, de ecuación

$$y = 2\,x$$




***Ejemplo 8-7.***

En el ejemplo 5-8 está comprobado que el conjunto $\mathbf{R}^{n \times m}$ de las matrices reales de $n$ filas y $m$ columnas, con la adición de matrices, es un grupo abeliano. En particular, si $m = n$, las matrices se llaman cuadradas, y se tiene que $(\mathbf{R}^{n \times n}\ , +)$, es el grupo abeliano de las matrices cuadradas $n \times n$, con la adición.

Consideremos el conjunto H de las matrices cuadradas, tales que $a_{i\,j} = a_{j\,i}$, llamadas simétricas, es decir

$$\mathrm{H} = \left\{ \mathrm{A} \in \mathbf{R}^{n \times n} \;/\; a_{ij} = a_{ji} \right\}$$

Esto significa que los elementos que son simétricos respecto de la diagonal $a_{i\,i}$, con $i = 1, 2, \ldots, n$, son iguales.

Resulta $(\mathrm{H}\ , +)$ un subgrupo de $(\mathbf{R}^{n \times n}, +)$. En efecto

i ) La matriz nula $\mathrm{N} \in \mathrm{H} \Rightarrow \mathrm{H} \neq \phi$

ii ) $\mathrm{H} \subset \mathbf{R}^{n \times n}$ por definición de H.

iii) Sean

$$\mathrm{A} \in \mathrm{H} \;\wedge\; \mathrm{B} \in \mathrm{H} \Rightarrow a_{ij} = a_{ji} \;\wedge\; b_{ij} = b_{ji} \Rightarrow$$
$$\Rightarrow a_{ij} - b_{ij} = a_{ji} - b_{ji} \Rightarrow \mathrm{A} + (-\,\mathrm{B}) \in \mathrm{H}$$

Hemos aplicado la definición de H, la sustracción en **R** y las definiciones de suma de matrices y de matriz opuesta.

(H , +) es el subgrupo de matrices simétricas $n \times n$.

*Ejemplo 8-8.*

Sean (G , $*$) un grupo, $a$ un elemento fijo de G, y H el conjunto de los elementos de G que conmutan con $a$, es decir

$$H = \left\{ x \in G \,/\, a * x = x * a \right\}$$

Resulta H un subgrupo de (G , $*$).

i ) como $a * e = e * a \Rightarrow e \in H \Rightarrow H \neq \phi$

ii ) $H \subset G$ por definición de H.

iii) Sean $m$ y $n$ elementos de H. Debemos probar que $m * n' \in H$.
Por definición de H

$$m \in H \ \wedge \ n \in H \Rightarrow a * m = m * a \ \wedge \ a * n = n * a \Rightarrow$$
$$\Rightarrow a * m = m * a \ \wedge \ n' * a' = a' * n' \Rightarrow$$
$$\Rightarrow (a * m) * (n' * a') = (m * a) * (a' * n') \Rightarrow$$
$$\Rightarrow a * (m * n') * a' = m * (a * a') * n' \Rightarrow$$
$$\Rightarrow a * (m * n') * a' = m * n' \Rightarrow$$
$$\Rightarrow a * (m * n') = (m * n') * a \Rightarrow$$
$$\Rightarrow m * n' \in H.$$

Además de la definición de H hemos utilizado inverso de la composición, la asociatividad, $G_4$, y la composición a derecha con $a$.

## 8.5. OPERACIONES CON SUBGRUPOS

### 8.5.1. Intersección de subgrupos

Sean (G , $*$) un grupo, y $\left\{G_i\right\}_{i \in I}$ una familia de subgrupos de (G , $*$).

***Teorema***

La intersección de toda familia no vacía de subgrupos de (G , $*$) es un subgrupo.

Hipótesis) (G , $*$) es grupo.

$\left\{G_i\right\}$ es tal que $(G_i , *)$ es subgrupo de G, $\forall\, i \in I$

Tesis) $\left( \bigcap\limits_{i \in I} G_i \, , * \right)$ es subgrupo de (G , $*$)

Demostración)

i ) $\forall i : e \in G_i$, pues $(G_i , *)$ es grupo
entonces, por definición de intersección

$$e \in \bigcap_{i \in I} G_i \Rightarrow \bigcap_{i \in I} G_i \neq \phi$$

ii ) $\bigcap_{i \in I} G_i \subset G$ por definición de inclusión

iii) Sean

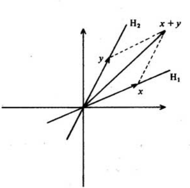
$$a \ \text{y} \ b \in \bigcap_{i \in I} G_i \Rightarrow a \in G_i \ \wedge \ b \in G_i , \forall i \Rightarrow$$

$$\Rightarrow a * b' \in G_i , \forall i \Rightarrow a * b' \in \bigcap_{i \in I} G_i$$

Por las definiciones de intersección y de subgrupos.

### 8.5.2. Unión de subgrupos

La propiedad anterior no se verifica en el caso de la unión. Para ello basta un contraejemplo: sean $H_1$ y $H_2$ dos subgrupos distintos de $(\mathbf{R}^2 , +)$, y no triviales, como lo muestra la figura




Si $x \in H_1 \ \wedge \ y \in H_2$, entonces

$$x \in H_1 \cup H_2 \ \wedge \ y \in H_1 \cup H_2$$

y sin embargo

$$x + y \notin H_1 \cup H_2$$

Es decir, la unión no es cerrada para la suma de pares, y por lo tanto no es subgrupo de $(\mathbf{R}^2, +)$.

***Ejemplo 8-9.***

Sean $(G', *)$ y $(G'', *')$ grupos. En el producto cartesiano

$$G = G' \times G''$$

se define la ley de composición "$\bullet$" mediante

$$(a, b) \bullet (c, d) = (a * c, b *' d) \qquad (1)$$

Entonces $(G, \bullet)$ es un grupo, llamado producto de los dados.

Verificamos los axiomas:

$G_1$ . $\bullet$ es ley interna en $G = G' \times G''$ por (1)

$G_2$ . $\bullet$ es asociativa, pues

$$[(a, b) \bullet (c, d)] \bullet (e, f) = (a * c, b *' d) \bullet (e, f) =$$
$$= ((a * c) * e, (b *' d) *' f) = (a * (c * e), b *' (d *' f)) =$$
$$= (a, b) \bullet (c * e, d *' f) = (a, b) \bullet [(c, d) \bullet (e, f)]$$

Hemos utilizado sucesivamente: la definición (1), $G_2$ en G' y G", y la definición (1).

$G_3$ . Neutro es $(e', e'')$, es decir, el par ordenado de los neutros de G' y de G".

En efecto, por (1) y $G_3$ en G' y G"

$$(a, b) \bullet (e', e'') = (e', e'') \bullet (a, b) = (a, b)$$

$G_4$ . Inverso de $(a, b)$ es $(a^{-1}, b^{-1})$, donde $a^{-1}$ y $b^{-1}$ son los inversos de $a$ y $b$ en G' y G" respectivamente, pues

$$(a, b) \bullet (a^{-1}, b^{-1}) = (a^{-1}, b^{-1}) \bullet (a, b) = (e', e'')$$

## 8.6. HOMOMORFISMOS DE GRUPOS

### 8.6.1. Concepto

Retomamos, en el caso particular de las estructuras de grupo, lo expuesto en 5.4. en relación con los morfismos.

Sean ahora los grupos $(G, *)$ y $(G', *')$.

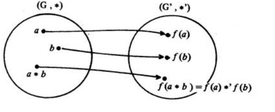
***Definición***

La función $f : G \to G'$ es un homomorfismo si y sólo si la imagen de la composición en G es igual a la composición de las imágenes en G'.

En símbolos

$$f : G \to G' \text{ es homomorfismo} \Leftrightarrow f(a * b) = f(a) *' f(b)$$

En un diagrama




En particular, el morfismo puede ser monomorfismo, epimorfismo, endomorfismo, isomorfismo o automorfismo, de acuerdo con las definiciones 5.4.2.

***Ejemplo 8-10.***

Sean los grupos aditivos $(\mathbf{R}^{2\times 2}, +)$ y $(\mathbf{R}, +)$.

La función $f : \mathbf{R}^{2\times 2} \to \mathbf{R}$ definida por

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + d \text{ es un homomorfismo, pues}$$

$$f(\mathrm{A} + \mathrm{B}) = f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} m & n \\ p & q \end{bmatrix}\right) =$$

$$= f\left(\begin{bmatrix} a+m & b+n \\ c+p & d+q \end{bmatrix}\right) = a + m + d + q =$$

$$= (a + d) + (m + q) = f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) + f\left(\begin{bmatrix} m & n \\ p & q \end{bmatrix}\right) =$$

$$= f(\mathrm{A}) + f(\mathrm{B}).$$

Hemos aplicado la definición de suma de matrices, de $f$, conmutatividad y asociatividad de la suma en $\mathbf{R}$ y la definición de $f$.

### 8.6.2. Propiedad

Si $f : \mathrm{G} \to \mathrm{G}'$ es un homomorfismo de grupos, entonces la imagen del neutro del primer grupo es el neutro del segundo grupo.

Se trata de probar que $f(e) = e'$, donde $e'$ denota el neutro de G'.

En efecto cualquiera que sea $x \in \mathrm{G}$, por $\mathrm{G}_3$, se tiene

$$x * e = x$$

Entonces

$$f(x * e) = f(x)$$

Por definición de homorfismo

$$f(x) *' f(e) = f(x)$$

Por $G_3$ en el grupo (G' , *')

$$f(x) *' f(e) = f(x) *' e'$$

Y por ley cancelativa en G' resulta

$$f(e) = e'$$

### 8.6.3. Propiedad

Si $f : G \to G'$ es un homomorfismo de grupos, entonces la imagen del inverso de todo elemento de G es igual al inverso de su imagen.

Es decir

$$f(x^{-1}) = [f(x)]^{-1}$$

Cualquiera que sea $x$ en G, por $G_4$

$$x * x^{-1} = e$$

Entonces

$$f(x * x^{-1}) = f(e)$$

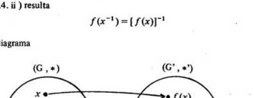
Por definición de homomorfismo y por 8.6.2. se tiene

$$f(x) *' f(x^{-1}) \quad e$$

Por 8.3.4. ii ) resulta

$$f(x^{-1}) = [f(x)]^{-1}$$

En un diagrama



## 8.7. NUCLEO E IMAGEN DE UN HOMOMORFISMO DE GRUPOS

### 8.7.1. Núcleo de un homomorfismo de grupos

Sea $f : G \to G'$ un morfismo de grupos. La determinación de los elementos del primer grupo, cuyas imágenes por $f$ son el neutro del segundo grupo, conduce a un subconjunto de G, llamado núcleo del homomorfismo.

***Definición***

Núcleo del homomorfismo $f : G \to G'$ es la totalidad de los elementos de G, cuyas imágenes por $f$ se identifican con el neutro de G'.

Es decir

$$N(f) = \left\{ x \in G \,/\, f(x) = e' \right\}$$

Es claro que el núcleo de $f$ es la preimagen de $\left\{ e' \right\}$

De acuerdo con la definición, se tiene

$$x \in N(f) \Leftrightarrow f(x) = e'$$

Esto significa que para verificar que un elemento pertenece al núcleo es suficiente probar que su imagen es $e'$.

*Ejemplo 8-11.*

El núcleo del homomorfismo del ejemplo 8-10 consiste en las matrices 2×2 tales que

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + d = 0\,, \quad \text{es decir } d = -a$$

En consecuencia, al núcleo de $f$ pertenecen todas las matrices del tipo

$$\begin{bmatrix} a & b \\ c & -a \end{bmatrix}$$

En este caso, los elementos de la diagonal son opuestos, o de suma cero, o de traza nula, siendo por definición la traza de una matriz la suma de los elementos de la diagonal. En general, la notación para la traza de una matriz $A \in R^{n \times n}$ es

$$\text{tr}\, A = \sum_{i=1}^{n} a_{ii}$$

### 8.7.2. Propiedad

El núcleo de todo homomorfismo de grupos es un subgrupo del primero.

Hipótesis) $(G\,,*)$ y $(G'\,,*')$ son grupos.

$f : G \to G'$ es un homomorfismo.

Tesis) (N ( $f$ ) , $*$) es subgrupo de (G , $*$).
Demostración)

i ) Por 8.6.2. $f(e)=e' \Rightarrow e \in N(f) \Rightarrow N(f) \neq \phi$

ii ) $N(f) \subset G$ por definición de núcleo.

iii) Sean

$$a \text{ y } b \in N(f) \Rightarrow f(a)=e' \wedge f(b)=e' \Rightarrow$$
$$\Rightarrow f(a)=e' \wedge [f(b)]^{-1}=e'^{-1} \Rightarrow$$
$$\Rightarrow f(a)=e' \wedge f(b^{-1})=e' \Rightarrow f(a) *' f(b^{-1})=e' \Rightarrow$$
$$\Rightarrow f(a*b^{-1})=e' \Rightarrow a*b^{-1} \in N(f)$$

Por definición de núcleo, imagen del inverso (8.6.3.), inverso del neutro, composición en G', homomorfismo y definición de núcleo.

En virtud de la condición suficiente 8.4.2., resulta (N ($f$), $*$) un subgrupo de (G , $*$).

### 8.7.3. Propiedad

El homomorfismo $f: G \to G'$ es inyectivo, es decir, un monomorfismo si y sólo si el núcleo es unitario.

Sea N ($f$) el núcleo del homomorfismo $f: G \to G'$

i ) $f$ es $1-1 \Rightarrow N(f)=\{e\}$

La demostración es inmediata, porque si en el núcleo hubiera otro elemento distinto de $e$, entonces dos elementos distintos de G tendrían la misma imagen por $f$, y no sería una función inyectiva.

ii ) $N(f)=\{e\} \Rightarrow f$ es $1-1$.

En efecto, sean $x$, $y \in G$ tales que $f(x)=f(y)$.
Componiendo con el inverso de $f(y)$, en G'

$$f(x) *' [f(y)]^{-1} = f(y) *' [f(y)]^{-1}$$

Por 8.6.3., y por $G_4$ en (G' , $*'$)

$$f(x) *' f(y^{-1})=e'$$

Por definición de homomorfismo

$$f(x*y^{-1})=e'$$

Por definición de núcleo

$$x*y^{-1} \in N(f)$$

Por ser $N(f)=\{e\}$ resulta

$$x*y^{-1}=e$$

Componiendo a derecha con $y$ ·

$$x * y^{-1} * y = e * y$$

O sea

$$x = y$$

y $f$ es inyectiva.

### 8.7.4. Imagen de un homomorfismo de grupos

Sea $f: G \to G'$ un morfismo de grupos.

***Definición***

Imagen de un morfismo de grupos es la totalidad de las imágenes de los elementos del primer grupo.

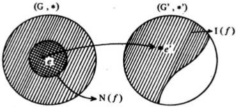
La imagen de un morfismo de grupos es la imagen de la función que lo define, es decir

$$I(f) = \left\{ f(x) \in G' \,/\, x \in G \right\}$$

O bien

$$I(f) = \left\{ y \in G' \,/\, \exists\, x \in G \;\wedge\; f(x) = y \right\}$$

Es claro que si el morfismo es un epimorfismo, es decir, si $f$ es sobreyectiva, entonces $I(f) = G'$. En el siguiente diagrama se tiene una representación de $N(f)$ y de $I(f)$




En el caso del ejemplo 8-10, $f$ es un epimorfismo, pero no es monomorfismo.

### 8.7.5. Propiedad

La imagen de todo homomorfismo de grupos es un subgrupo del segundo.
Hipótesis) (G , $*$) y (G' , $*'$) son grupos.

$$f: G \to G' \text{ es un homomorfismo.}$$

Tesis) (I ($f$) , $*'$) es subgrupo de (G , $*$)
Demostración)

i ) Como $f(e) = e' \Rightarrow e' \in I(f) \Rightarrow I(f) \neq \phi$

ii ) $I(f) \subset G'$ por definición de $I(f)$

iii) Sean $y_1 \wedge y_2 \in I(f)$

Entonces, por definición de imagen, $\exists\, x_1$ y $x_2$ en G, tales que

$$f(x_1) = y_1 \wedge f(x_2) = y_2$$

Por inversos en G'

$$f(x_1) = y_1 \wedge [f(x_2)]^{-1} = y_2^{-1}$$

Por inverso de la imagen

$$f(x_1) = y_1 \wedge f(x_2^{-1}) = y_2^{-1}$$

Por composición en G'

$$f(x_1) *' f(x_2^{-1}) = y_1 *' y_2^{-1}$$

Por homomorfismo

$$f(x_1 * x_2^{-1}) = y_1 *' y_2^{-1}$$

y como $x_1 * x_2^{-1} \in G$, por definición de imagen, se tiene

$$y_1 *' y_2^{-1} \in I(f)$$

En consecuencia, según 8.4.2., resulta que

$$(I(f), *')$$

es un subgrupo de (G' , $*'$)

*Ejemplo 8-12.*

Sea $G_3$ el conjunto de las tres raíces cúbicas de la unidad, es decir, de las soluciones complejas de la ecuación

$$x^3 - 1 = 0$$

El factoreo del primer miembro conduce a

$$(x - 1) \cdot (x^2 + x + 1) = 0$$

Entonces

$$x-1=0 \text{ ó } x^2+x+1=0$$

La resolución de estas ecuaciones conduce a las tres raíces cúbicas de 1:

$$x_1 = 1 \qquad x_2 = -\frac{1}{2} + i\,\frac{\sqrt{3}}{2} \qquad x_3 = -\frac{1}{2} - i\,\frac{\sqrt{3}}{2}$$

que llamamos, respectivamente, $z_0, z_1$ y $z_2$. En el capítulo 11 veremos que las $n$ raíces $n$-simas de la unidad están dadas por la fórmula

$$z_k = \cos\frac{2\,k\,\pi}{n} + i \operatorname{sen}\frac{2\,k\,\pi}{n} = e^{\,i\frac{2k\pi}{n}}$$

donde $k$ toma los valores enteros $0, 1, 2, \ldots, n-1$.

En el caso particular de las raíces cúbicas, la fórmula anterior adopta la expresión

$$z_k = \cos\frac{2\,k\,\pi}{3} + i \operatorname{sen}\frac{2\,k\,\pi}{3} = e^{\,i\frac{2k\pi}{3}}$$

donde $k = 0, 1, 2$. Por definición de raíz cúbica se verifica

$$z_h \in G_3 \Leftrightarrow z_h^3 = 1$$

Nos proponemos probar que $G_3$ es un grupo multiplicativo abeliano, y además obtener un método para el producto.

i ) $(G_3\,, .)$ es grupo conmutativo.

I) El producto es ley interna en $G_3$. En efecto

$$z_h \in G_3 \;\wedge\; z_l \in G_3 \Rightarrow z_h^3 = 1 \;\wedge\; z_l^3 = 1 \Rightarrow z_h^3 \,.\, z_l^3 = 1 \Rightarrow$$

$$\Rightarrow (z_h\,.\,z_l)^3 = 1 \Rightarrow z_h\,.\,z_l \in G_3$$

II) El producto es asociativo en $G_3$. Aquí nada hay que demostrar, pues $G_3 \subset \mathbf{C}$, y el producto es asociativo en $\mathbf{C}$.

III) Existe neutro para el producto en $G_3$, y es

$$z_0 = \cos 0 + i \operatorname{sen} 0 = 1$$

IV) Todo elemento de $G_3$ tiene inverso multiplicativo en $G_3$.

$$\text{Sea } \; z_h \in G_3 \Rightarrow z_h^3 = 1 \Rightarrow \left(z_h^3\right)^{-1} = 1 \Rightarrow$$

$$\Rightarrow \left(z_h^{-1}\right)^3 = 1 \Rightarrow z_h^{-1} \in G_3$$

V) El producto es conmutativo en $G_3$, por serlo en $\mathbf{C}$.

ii ) Vamos a establecer un método para obtener el producto de dos raíces cúbicas de la unidad.

**Sean**

$$z_l \in G_3 \wedge z_m \in G_3 \Rightarrow$$
$$\Rightarrow z_l = e^{i\frac{2l\pi}{3}} \wedge z_m = e^{i\frac{2m\pi}{3}}$$

**donde**

$$0 \leq l < 3 \wedge 0 \leq m < 3$$

**Entonces**

$$z_l \,.\, z_m = e^{i\frac{2(l+m)\pi}{3}} \qquad (1)$$

Si dividimos $l + m$ por 3, se obtienen $q$ y $r$, únicos, tales que

$$\left.\begin{array}{l} l + m = 3q + r \\ 0 \leq r < 3 \end{array}\right\} \qquad (2)$$

De (1) y (2)

$$z_l \,.\, z_m = e^{i\frac{2(3q+r)\pi}{3}} = e^{i2q\pi} \,.\, e^{i\frac{2r\pi}{3}} =$$
$$= (\cos 2q\pi + i \operatorname{sen} 2q\pi) \,.\, e^{i\frac{2r\pi}{3}} = 1 \,.\, e^{i\frac{2r\pi}{3}} =$$
$$= e^{i\frac{2r\pi}{3}} = z_r \quad \text{donde } 0 \leq r < 3$$

La tabla de la composición es, entonces

| | $z_0$ | $z_1$ | $z_2$ |
|---|---|---|---|
| $z_0$ | $z_0$ | $z_1$ | $z_2$ |
| $z_1$ | $z_1$ | $z_2$ | $z_0$ |
| $z_2$ | $z_2$ | $z_0$ | $z_1$ |

***Ejemplo 8-13.***

Sean los grupos $(\mathbf{Z}, +)$ y $(G_3, .)$, y la función

$$f : \mathbf{Z} \to G_3 \quad \text{definida por la asignación}$$

$f(x) = z_r$, siendo $r$ el resto de la división de $x$ por 3, es decir, el entero no negativo que satisface las condiciones

$$\begin{cases} x = 3 \,.\, q + r \\ 0 \leq r < 3 \end{cases}$$

Vamos a probar que tal aplicación es un homomorfismo, es decir

$$f(x' + x'') = f(x') \,.\, f(x'')$$

Por la definición de $f$

$$(1)\begin{cases} f(x')=z_{r'} \\ f(x'')=z_{r''} \\ f(x'+x'')=z_r \quad \text{donde} \end{cases}$$

$$(2)\begin{cases} x'=3\,q'+r' & \wedge \quad 0\leqslant r'<3 \\ x''=3\,q''+r'' & \wedge \quad 0\leqslant r''<3 \\ x'+x''=3\,q+r & \wedge \quad 0\leqslant r<3 \end{cases}$$

Por ser $(G_3\,,\,\cdot\,)$ un grupo, de acuerdo con el ejemplo 8-12, tenemos

$$z_{r'}\,.\,z_{r''}=z_{r'''} \quad \text{siendo}$$
$$r'+r''=3\,q'''+r''' \;\wedge\; 0\leqslant r'''<3 \qquad (3)$$

Sumando las dos primeras relaciones de (2)

$$x'+x''=3\,(q'+q'')+(r'+r'') \qquad (4)$$

Por (3) y (4)

$$x'+x''=3\,(q'+q'')+3\,q'''+r''' \Rightarrow$$
$$\Rightarrow x'+x''=3\,(q'+q''+q''')+r''' \;\wedge\; 0\leqslant r'''<3 \qquad (5)$$

Por la unicidad del cociente y resto, de (5) y de la última igualdad que figura en (2) se tiene

$$q=q'+q''+q''' \;\wedge\; r=r'''$$

Es decir

$$z_{r'''}=z_r$$

Se verifica entonces

$$f(x'+x'')=z_r=z_{r'''}=z_{r'}\,.\,z_{r''}=f(x')\,.\,f(x'')$$

y el homomorfismo está probado.

***Ejemplo 8-14.***

Determinaremos el núcleo y la imagen del homomorfismo del ejemplo anterior.

$$x\in \mathbf{Z} \Rightarrow \exists\, q \;\wedge\; r \text{ únicos} \,/\, x=3\,q+r \;\wedge\; 0\leqslant r<3$$

Por definición de $f$

$$f(x)=z_r$$

Por definición de $N(f)$

$$x\in N(f) \Leftrightarrow f(x)=z_o=1 \Leftrightarrow r=0$$

Luego

$$x \in \mathrm{N}(f) \Leftrightarrow x = 3\,q \Leftrightarrow 3 \mid x$$

Es decir

$$\mathrm{N}(f) = \left\{ x \in z \;/\; 3 \mid x \right\}$$

Por otra parte, obviamente, es $\mathrm{I}(f) = \mathrm{G}_3$ y el homomorfismo es un epimorfismo.

*Ejemplo 8-15.*

Verificar que los grupos $(\mathrm{G}_3\,,\,.)$ y $(R\,,\circ)$ son isomorfos, siendo $R$ el conjunto de las rotaciones del triángulo equilátero, alrededor del centro, que llevan la figura sobre sí misma.

En $R$ se tienen las rotaciones $R_0$, $R_1$ y $R_2$, que son la identidad, y las rotaciones de 120° y 240°.

En $\mathrm{G}_3$, los elementos son $z_0$, $z_1$ y $z_2$, con el significado dado en los ejemplos anteriores.

La función $f : \mathrm{G}_3 \to R$, tal que

$$f(z_i) = R_i$$

es un isomorfismo respecto del producto en $\mathrm{G}_3$ y de la composición en $R$ pues

$$f(z_l \,.\, z_m) = f(r) = R_r$$

## 8.8. RELACION DE EQUIVALENCIA COMPATIBLE

### 8.8.1. Concepto

Sean $(\mathrm{G}\,,*)$ un grupo, y "$\sim$" una relación de equivalencia en G.

La definición 5.5. establece que $\sim$ es compatible con $*$ si y sólo si

$$a \sim b \;\wedge\; c \sim d \;\Rightarrow\; a * c \sim b * d$$

### 8.8.2. Teorema fundamental de compatibilidad

Si $\sim$ es una relación de equivalencia compatible con la ley interna del grupo $(\mathrm{G}\,,*)$, entonces existe en el conjunto cociente $\frac{\mathrm{G}}{\sim}$ una única ley de composición interna $*'$, tal que la aplicación canónica $f : \mathrm{G} \to \frac{\mathrm{G}}{\sim}$ es un homomorfismo, y además $\left(\frac{\mathrm{G}}{\sim}\,,*'\right)$ es grupo.

Este teorema es un corolario de lo demostrado en 5.5.1.

***Definición***

El grupo $\frac{G}{\sim}$ a que se refiere el teorema se llama grupo cociente de G por la relación de equivalencia compatible con $*$.

***Ejemplo 8-16.***

Consideremos el grupo aditivo de las clases de restos módulo $n$. En este caso

$$\mathbf{Z}_n = \left\{ \overline{0}, \overline{1}, \ldots, \overline{n-1} \right\}$$

De acuerdo con el ejemplo 5-12, se sabe que la congruencia módulo $n$ es compatible con la adición en $\mathbf{Z}$; entonces, por el teorema fundamental de compatibilidad, se tiene en el conjunto cociente $\mathbf{Z}_3$ una única ley de composición interna inducida, llamada suma de clases, tal que la aplicación canónica $f : \mathbf{Z} \to \mathbf{Z}_n$ es un homomorfismo, siendo $(\mathbf{Z}_n, \oplus)$ el grupo aditivo de las clases de restos módulo $n$.

Para sumar dos clases en $\mathbf{Z}_n$ procedemos así

$$\overline{u} \oplus \overline{v} = f(u) \oplus f(v) = f(u+v) \qquad (1)$$

Dividiendo $u + v$ y $n$ se obtienen $q$ y $r$, tales que

$$u + v = n\,q + r \ \wedge \ 0 \leqslant r < n \qquad (2)$$

De (2) y (1)

$$\overline{u} \oplus \overline{v} = f(n\,q + r) = f(r) = \overline{r}$$

ya que

$$(u+v) - r = n\,q \Rightarrow n|(u+v) - r \Rightarrow$$
$$\Rightarrow u + v \sim r$$

## 8.9. SUBGRUPOS DISTINGUIDOS

### 8.9.1. Concepto

Sean $(\mathbf{Z}, +)$ el grupo aditivo de los enteros y el subconjunto H de los múltiplos de 3, es decir

$$\mathrm{H} = \left\{ x \in \mathbf{Z} \,/\, 3 \,|\, x \right\}$$

Si consideramos la congruencia módulo 3 en $\mathbf{Z}$, entonces la aplicación canónica

$$f : \mathbf{Z} \to \mathbf{Z}_3$$

es un homomorfismo de $(\mathbf{Z}, +)$ en $(\mathbf{Z}_3, +)$ cuyo núcleo es, precisamente, H. En este caso, decimos que H es un subgrupo distinguido de G.

***Definición***

El subgrupo $(H, *)$ de $(G, *)$ es distinguido si y sólo si existe un grupo $(G', *')$ y un homomorfismo $f: G \to G'$, cuyo núcleo es H.

En símbolos

$H \subset G$ es distinguido $\Leftrightarrow \exists\, G'$ grupo, y $f: G \to G'$ homomofismo / $N(f) = H$

Subgrupos distinguidos de todo grupo $(G, *)$ son el mismo G y $\{e\}$. En efecto, en el primer caso, la aplicación

$$f: G \to G \quad \text{definida por } f(x) = e \quad \text{para todo } x \in G,$$

es un homomorfismo, ya que

$$f(a * b) = e = e * e = f(a) * f(b)$$

Además, se verifica que $N(f) = G$.

En el segundo caso, basta definir $f: G \to G$ mediante $f(x) = x$, cualquiera que sea $x$ en G, y se tiene un homomorfismo, pues

$$f(a * b) = a * b = f(a) * f(b)$$

y como $N(f) = \{e\}$, resulta $\{e\}$ un subgrupo distinguido de G.

Sean ahora un grupo $(G, *)$ y $\sim$ una relación de equivalencia compatible con $*$. Por el teorema fundamental de compatibilidad sabemos que $\left(\frac{G}{\sim}, *'\right)$ es el grupo cociente de G por la equivalencia, y que la aplicación canónica

$$f: G \to \frac{G}{\sim}$$

es un homomorfismo respecto de $*$ y $*'$. Por lo que antecede es obvio que el subgrupo $(N(f), *)$ es distinguido, y queda caracterizado en términos de la relación de equivalencia compatible con la ley del grupo G. Existe una estrecha conexión entre las relaciones de equivalencia compatibles con la ley de composición interna de un grupo y los subgrupos distinguidos de éste. El teorema que sigue aclara la situación.

8.9.2. **Teorema.** El conjunto $\mathbb{E}$ de todas las relaciones de equivalencia definidas en G, compatibles con la ley interna del grupo $(G, *)$, es coordinable al conjunto $\mathbb{G}$ de todos los subgrupos distinguidos de $(G, *)$.

Hipótesis) $(G, *)$ es grupo

$$\mathbb{E} = \left\{ \mathcal{E}_i \,/\, \mathcal{E}_i \text{ es de equivalencia en G, compatible con } * \right\}$$

$$\mathbb{G} = \left\{ H_i \,/\, H_i \text{ es subgrupo distinguido de G} \right\}$$

Tesis) $\mathbb{E}$ es coordinable a $\mathbb{G}$

Demostración)

Definimos $\Phi: \mathbb{E} \to \mathbb{G}$ mediante la asignación

$$\Phi(\mathcal{E}_i) = N(f_i). \quad (1)$$

siendo $N(f_i)$ el núcleo del homomorfismo $f_i : G \to \frac{G}{\mathcal{E}_i}$ asociado a la equivalencia $\mathcal{E}_i$. Debemos probar que $\Phi$ es biyectiva.

i) Inyectividad.

Sean $\mathcal{E}_i$ y $\mathcal{E}_j \in \mathbb{E}$ tales que $\mathcal{E}_i \neq \mathcal{E}_j$.

Como $\mathcal{E}_i$ y $\mathcal{E}_j$ son subconjuntos distintos de $G^2$, existe $(x, y) \in G^2$ tal que

$$(x, y) \in \mathcal{E}_i \ \wedge \ (x, y) \notin \mathcal{E}_j$$

o bien

$$(x, y) \notin \mathcal{E}_i \ \wedge \ (x, y) \in \mathcal{E}_j$$

Razonamos sobre el primer caso, es decir, suponiendo

$$x\, \mathcal{E}_i\, y \ \wedge \ x \not\mathcal{E}_j\, y$$

por la compatibilidad de las relaciones de equivalencia, componiendo a izquierda con $y^{-1}$

$$(y^{-1} * x)\, \mathcal{E}_i\, (y^{-1} * y) \ \wedge \ (y^{-1} * x) \not\mathcal{E}_j\, (y^{-1} * y)$$

Entonces, por $G_4$

$$(y^{-1} * x)\, \mathcal{E}_i\, e \ \wedge \ (y^{-1} * x) \not\mathcal{E}_j\, e$$

Por definición de aplicación canónica e imagen del neutro

$$f_i(y^{-1} * x) = f_i(e) = e' \ \wedge \ f_j(y^{-1} * x) \neq f_j(e) = e'$$

Por definición de núcleo resulta

$$(y^{-1} * x) \in N(f_i) \ \wedge \ (y^{-1} * x) \notin N(f_j)$$

Es decir

$$N(f_i) \neq N(f_j)$$

Y de acuerdo con (1) se tiene

$$\Phi(\mathcal{E}_i) \neq \Phi(\mathcal{E}_j)$$

En consecuencia $\Phi$ es inyectiva.

ii) Sobreyectividad

Sea $H \in \mathbb{G}$, es decir, un subgrupo distinguido de $(G, *)$. Entonces, por definición, existe un grupo $(G', *')$ y un homomorfismo

$$f : G \to G' \text{ tal que}$$

$$N(f) = H = \left\{ x \in G \ / \ f(x) = e' \right\}$$

Se trata de probar que existe $\mathcal{E} \in \mathbb{E}$, tal que

$$\Phi(\mathcal{E}) = H$$

Para esto definimos la siguiente relación de equivalencia en G

$$x_1 \; \mathcal{E} \; x_2 \Leftrightarrow f(x_1) = f(x_2) \qquad (1)$$

$\mathcal{E}$ es compatible con $*$, pues

$$x_1 \; \mathcal{E} \; x_2 \; \wedge \; y_1 \; \mathcal{E} \; y_2 \Rightarrow f(x_1) = f(x_2) \; \wedge \; f(y_1) = f(y_2) \Rightarrow$$
$$\Rightarrow f(x_1) *' f(y_1) = f(x_2) *' f(y_2) \Rightarrow$$
$$\Rightarrow f(x_1 * y_1) = f(x_2 * y_2)$$

por composición en G' y por ser $f$ un homomorfismo.

Por (1) resulta

$$(x_1 * y_1) \; \mathcal{E} \; (x_2 * y_2)$$

Es decir: $\mathcal{E} \in \mathbf{E}$, y se verifica

$$\Phi(\mathcal{E}) = \mathrm{N}(f) = \mathrm{H}.$$

Entonces $\Phi$ es sobreyectiva.

De i ) y ii ) $\Phi$ resulta biyectiva, y en consecuencia

$$\mathbf{E} \sim \mathbb{G}$$

*Notación*

Si $\mathcal{E}$ es una relación de equivalencia compatible con la ley del grupo (G , $*$), y H el subgrupo distinguido asociado, escribimos $\dfrac{G}{\mathcal{E}} = \dfrac{G}{H}$, y se tiene el cociente de G por el subgrupo distinguido H.

***Ejemplo 8-17.***

Investigamos los subgrupos distinguidos de (**Z** , +). Si H es un subgrupo distinguido genérico, de acuerdo con la definición, existen un grupo G' y un homomorfismo

$$f : \mathbf{Z} \to G' \;\; \text{tal que} \;\; \mathrm{N}(f) = \mathrm{H}$$

Una posibilidad es $\mathrm{H} = \{0\}$ según 8.9.1.

Si $\mathrm{H} \neq \{0\}$, entonces existe $x \neq 0$, tal que $x \in \mathrm{H}$, y resulta $0 - x = -x \in \mathrm{H}$, es decir, en todo subgrupo no unitario de **Z** coexisten los elementos no nulos $x$ y $-x$, lo que significa que en H hay enteros positivos. Entonces, por el principio de buena ordenación, hay en H un elemento mínimo positivo, que llamamos $n$.

Consideramos ahora el conjunto A de todos los múltiplos enteros de $n$, y afirmamos que H = A. En efecto

i ) Sea $x \in \mathrm{H}$; lo dividimos por $n$ y se verifica

$$x = n \, . \, q + r \; \wedge \; 0 \leqslant r < n$$

Entonces $\qquad r = x - n \, . \, q \quad (1)$

Por definición, si $n \in \mathrm{N}$ y $q \in \mathrm{Z}$, entonces

$$n \cdot q = \underbrace{n + n + \ldots + n}_{q} \text{ si } q > 0$$

$$n \cdot q = \underbrace{(-n) + (-n) + \ldots + (-n)}_{q} \text{ si } q < 0$$

$$n \cdot q = 0 \text{ si } q = 0$$

Es decir, en todo caso $n \cdot q \in \mathrm{H}$, y por (1) resulta $r \in \mathrm{H}$, y siendo $n$ el mínimo entero positivo de H necesariamente es $r = 0$, es decir

$$x = n \cdot q \Rightarrow x \in \mathrm{A}$$

Así se tiene $\mathrm{H} \subset \mathrm{A}$.

ii ) Sea $x \in \mathrm{A}$. Por la definición de A se tiene $x = n \cdot m$ con $m \in \mathbf{Z}$.

Ahora bien

$$n \cdot m = \underbrace{n + n + \ldots + n}_{m} \text{ si } m > 0$$

$$n \cdot m = \underbrace{(-n) + (-n) + \ldots + (-n)}_{m} \text{ si } m < 0$$

$$n \cdot m = 0 \text{ si } m = 0$$

En todo caso, se verifica $x = n \cdot m \in \mathrm{H}$, es decir, $\mathrm{A} \subset \mathrm{H}$.

Luego $\mathrm{H} = \mathrm{A}$.

Esto significa que todo subgrupo distinguido de $(\mathbf{Z}, +)$ se identifica con el conjunto $\{0\}$, o bien con el conjunto de los múltiplos de un entero positivo.

## 8.10. SUBGRUPOS NORMALES O INVARIANTES

### 8.10.1. *Definición*

El subgrupo $(\mathrm{H}, *)$ de $(\mathrm{G}, *)$ es normal o invariante, si y sólo si se verifica

$$x \in \mathrm{G} \ \wedge \ y \in \mathrm{H} \Rightarrow x * y * x^{-1} \in \mathrm{H}$$

*Ejemplo 8-18.*

Todo subgrupo de un grupo conmutativo, es invariante.

Sea $(\mathrm{H}, *)$ un subgrupo de $(\mathrm{G}, *)$, y éste conmutativo. Entonces

$$\forall y \, \forall x : x \in G \;\wedge\; y \in H \Rightarrow x * y * x^{-1} = x * x^{-1} * y =$$
$$= e * y = y \in H$$

y por definición

$$(H, *) \text{ es invariante.}$$

**8.10.2. Teorema.** Un subgrupo es distinguido si y sólo si es invariante.

I) (H , *) es distinguido ⇒ (H , *) es invariante.

Sea $\sim$ la relación de equivalencia en G, compatible con $*$, asociada al subgrupo distinguido H. Entonces

$$H = N(f) = \left\{ x \in G \,/\, f(x) = e' \right\} = \left| \left\{ x \in G \,/\, x \sim e \right\} \right. \qquad (1)$$

Por (1)

$$y \in H \Rightarrow y \sim e$$

Por la compatibilidad

$$x \in G \Rightarrow x * y \sim x * e \Rightarrow x * y \sim x \Rightarrow$$
$$\Rightarrow x * y * x^{-1} \sim x * x^{-1} \Rightarrow x * y * x^{-1} \sim e \Rightarrow$$
$$\Rightarrow x * y * x^{-1} \in H$$

y en consecuencia (H , *) es distinguido.

II) (H , *) es invariante ⇒ (H , *) es distinguido.

Como (H , *) es invariante sabemos que

$$x \in G \;\wedge\; y \in H \Rightarrow x * y * x^{-1} \in H$$

a) Definimos en G la relación $\sim$ mediante

$$x_1 \sim x_2 \Leftrightarrow x_1 * x_2^{-1} \in H \;\wedge\; x_1^{-1} * x_2 \in H \qquad (2)$$

Se verifica:

i ) Reflexividad.

$$x \in G \Rightarrow x * x^{-1} \in H \;\wedge\; x^{-1} * x \in H \Rightarrow x \sim x$$

ii ) Simetría.

$$x_1 \sim x_2 \Rightarrow x_1 * x_2^{-1} \in H \;\wedge\; x_1^{-1} * x_2 \in H \Rightarrow$$
$$\Rightarrow x_2^{-1} * x_1 * x_2^{-1} * x_2 \in H \;\wedge\; x_2 * x_1^{-1} * x_2 * x_2^{-1} \in H \Rightarrow$$
$$\Rightarrow x_2 * x_1^{-1} \in H \;\wedge\; x_2^{-1} * x_1 \in H \Rightarrow x_2 \sim x_1$$

Por (2), por ser H invariante, por $G_4$ y definición (2).

iii) Transitividad

$$x_1 \sim x_2 \wedge x_2 \sim x_3 \Rightarrow$$
$$\Rightarrow x_1 * x_2^{-1} \in H \wedge x_1^{-1} * x_2 \in H \wedge x_2 * x_3^{-1} \in H \wedge x_2^{-1} * x_3 \in H \Rightarrow$$
$$\Rightarrow x_1 * x_2^{-1} * x_2 * x_3^{-1} \in H \wedge x_1^{-1} * x_2 * x_2^{-1} * x_3 \in H \Rightarrow$$
$$\Rightarrow x_1 * x_3^{-1} \in H \wedge x_1^{-1} * x_3 \in H \Rightarrow x_1 \sim x_3$$

Por (2), composición en H, $G_4$ y (2)

b) $\sim$ es compatible con $*$ en G, pues

$$x_1 \sim x_2 \Rightarrow x_1 * x_2^{-1} \in H \qquad (3) \qquad \text{Por (2)}$$
$$x_1' \sim x_2' \Rightarrow x_1' * x_2'^{-1} \in H \Rightarrow x_1 * (x_1' * x_2'^{-1}) * x_1^{-1} \in H \qquad (4)$$

Por (2) y por ser H invariante.

De (3) y (4)

$$x_1 * (x_1' * x_2'^{-1}) * x_1^{-1} * x_1 * x_2^{-1} \in H \Rightarrow$$
$$\Rightarrow x_1 * \left(x_1' * x_2'^{-1}\right) * x_2^{-1} \in H \Rightarrow$$
$$\Rightarrow (x_1 * x_1') * (x_2'^{-1} * x_2^{-1}) \in H \Rightarrow$$
$$\Rightarrow (x_1 * x_1') * (x_2 * x_2')^{-1} \in H$$

Por $G_4$, $G_2$, e inverso de la composición.

Análogamente se prueba que

$$(x_1 * x_1')^{-1} * (x_2 * x_2') \in H$$

Luego

$$x_1 * x'_1 \sim x_2 * x'_2$$

c) Como E es coordinable a G, existe un subgrupo distinguido G', asociado a $\sim$ tal que

$$G' = N(f) = \left\{x \in G \,/\, x \sim e\right\} = H$$

Luego H es distinguido.

## 8.11. GRUPO COCIENTE ASOCIADO A UN SUBGRUPO

### 8.11.1. Relación de equivalencia y coclases

Sea (H , $*$) un subgrupo de (G , $*$). Definimos en G la relación $\sim$ mediante.

$$a \sim b \Leftrightarrow a' * b \in H \qquad (1)$$

Es decir, dos elementos están relacionados si y sólo si la composición del inverso del primero con el segundo pertenece a H.

La relación (1) es de equivalencia pues verifica

i ) Reflexividad

$$a \in G \Rightarrow a' * a = e \in H \Rightarrow a \sim a$$

ii ) Simetría.

$$a \sim b \Rightarrow a' * b \in H \Rightarrow (a' * b)' \in H \Rightarrow b' * a \in H \Rightarrow b \sim a$$

De acuerdo con (1), por ser H un grupo, por inverso de la composición, inverso del inverso, y por (1).

iii) Transitividad.

$$a \sim b \ \wedge \ b \sim c \Rightarrow a' * b \in H \ \wedge \ b' * c \in H \Rightarrow a' * b * b' * c \in H \Rightarrow$$
$$\Rightarrow a' * c \in H \Rightarrow a \sim c$$

Por el teorema fundamental de las relaciones de equivalencia, existe una partición de G en clases de equivalencia, siendo

$$K_u = \left\{ x \in G \,/\, u \sim x \right\}$$

Ahora bien

$$u \sim x \Rightarrow u' * x = a \in H \Rightarrow x = u * a$$

En consecuencia

$$K_u = \left\{ x \in G \,/\, x = u * a \ \wedge \ a \in H \right\}$$

$K_u$ recibe el nombre de coclase a izquierda del subgrupo H en G. Si denotamos con los símbolos $u$H y H$u$ los conjuntos

$$uH = \left\{ u * x \,/\, x \in H \right\}$$
$$Hu = \left\{ x * u \,/\, x \in H \right\}$$

entonces es fácil verificar que $K_u = u$H, y el conjunto cociente $\frac{G}{H}$ es el de las coclases a izquierda de H en G.

### 8.11.2. Compatibilidad y grupo cociente

Sea H un subgrupo del grupo conmutativo G. La relación de equivalencia definida en G es compatible con la ley de composición $*$, pues

$$\begin{aligned} a \sim b \ \wedge \ c \sim d &\Rightarrow a' * b \in \mathrm{H} \ \wedge \ c' * d \in \mathrm{H} \Rightarrow \\ &\Rightarrow a' * b * c' * d \in \mathrm{H} \Rightarrow c' * a' * b * d \in \mathrm{H} \Rightarrow \\ &\Rightarrow (a * c)' * (b * d) \in \mathrm{H} \Rightarrow a * c \sim b * d \end{aligned}$$

De acuerdo con el teorema fundamental de compatibilidad, existe en $\frac{\mathrm{G}}{\mathrm{H}}$ una única ley de composición interna $*'$, tal que la aplicación canónica $f : \mathrm{G} \to \frac{\mathrm{G}}{\mathrm{H}}$ es un epimorfismo y $\left(\frac{\mathrm{G}}{\mathrm{H}}, *'\right)$ es un grupo conmutativo.

El conjunto $\frac{\mathrm{G}}{\mathrm{H}}$, dotado de la ley de composición inducida, se llama grupo cociente de G por la relación de equivalencia (1).

La manera de operar con las coclases es la siguiente:

$$(u\mathrm{H}) *' (v\mathrm{H}) = f(u) *' f(v) = f(u * v) = (u * v)\,\mathrm{H}$$

*Ejemplo 8-19.*

Sean el grupo abeliano $(\mathbf{R}^2 , +)$ y el subgrupo $\mathrm{H} = \left\{(x , x) \,/\, x \in \mathbf{R}\right\}$

Geométricamente, H corresponde a la bisectriz del primer cuadrante. La relación de equivalencia (1) se traduce en

$$(a , b) \sim (c , d) \Leftrightarrow (-a , -b) + (c , d) \in \mathrm{H} \Leftrightarrow (c , d) = (a , b) + (x , x)$$

Se tiene entonces

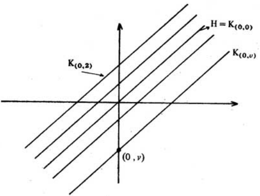
$$\mathrm{K}_{(a,b)} = (a , b)\,\mathrm{H} = \left\{(a + x , b + x) \,/\, x \in \mathbf{R}\right\}$$

Vamos a determinar la coclase de $(1 , 2) \in \mathbf{R}^2$. A ella pertenecen los pares $(x , y)$ que satisfacen $(x , y) = (1 , 2) + (a , a)$ con $a \in \mathbf{R}$. Resulta el sistema de ecuaciones paramétricas

$$x = 1 + a$$
$$y = 2 + a$$

y eliminando el parámetro $a$ se tiene $y - 2 = x - 1$, es decir, $y = x + 1$, que corresponde a la recta paralela a la primera bisectriz que pasa por el punto $(0 , 1)$.

El conjunto cociente, que representamos a continuación, consiste en el haz de rectas del plano cuya dirección coincide con la de la primera bisectriz. Un conjunto de índices es $\mathrm{I} = \left\{ (0 , \nu) \ / \ \nu \in \mathbf{R}\right\}$, o sea, el eje de ordenadas.




En el grupo cociente, la ley inducida es la suma de coclases, y se efectúa así

$$K_{(0,v)} + K_{(0,v')} = K_{(0,v+v')}$$

O bien

$$(0\,,\nu)\,H + (0\,,\nu')\,H = (0\,,\nu+\nu')\,H$$

Es claro que la coclase neutra es $K_{(0,0)} = H$ y la opuesta de $\nu H$ es $(-v)\,H$.

## 8.12. GRUPOS CICLICOS

### 8.12.1. Generadores de un grupo

Sea S una parte no vacía del grupo G.

***Definición***

Subgrupo generado por el conjunto no vacío $S \subset G$ es la intersección de todos los subgrupos que contienen a S.

Si $\overline{S}$ es el subgrupo generado por S, entonces podemos escribir

$$\overline{S} = \bigcap_{H_i \supset S} H_i$$

donde $H_i$ es un subgrupo de G que contiene a S.

Es claro que el subgrupo generado por S es el mínimo subgrupo, en el sentido de inclusión, que contiene a S.

Si $\overline{S} = G$, entonces se dice que S es un generador de G.

8.12.2. **Grupo cíclico**

Sea (G , *) un grupo.

*Definición*

El grupo G es cíclico si y sólo si es generado por un elemento.
Es decir

$$G \text{ es cíclico} \Leftrightarrow \exists a \in G \ / \ G = \overline{\{a\}}$$

Diremos que el grupo cíclico G, generado por $a$, es infinito si y sólo si no existe un entero positivo $m$ tal que $a^m = a * a * \ldots * a = e$.

Si $n$ es el menor entero positivo que verifica $a^n = e$, entonces el grupo G consiste en los $n$ elementos distintos

$$e \, , a \, , a^2 \, , \ldots \, , a^{n-1}$$

y se dice que es cíclico de orden $n$.

Es obvio que el subgrupo de (G , *), siendo G un grupo arbitrario, generado por $a \in G$, es cíclico.

*Definición*

El elemento $a \in G$ es de orden infinito si y sólo si el subgrupo generado por $a$ es infinito.

El elemento $a \in G$ es de orden $n$ (natural) si y sólo si el subgrupo generado por $a$ es de orden $n$.

*Ejemplo 8-20.*

i ) El grupo (Z , +) es cíclico, pues está generado por el entero 1, y su orden es infinito, pues no existe ningún número natural $n$ que verifique

$$\underbrace{1 + 1 + \ldots + 1}_{n} = 0$$

ii ) El grupo ($Z_n$ , +) es cíclico, ya que está generado por $\overline{1}$, y de orden $n$ pues

$$\underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{n} = \overline{0}.$$

## 8.13. TRASLACIONES DE UN GRUPO

Sea $a$ un elemento del grupo G.

*Definición*

Traslación a izquierda del grupo (G , *) por el elemento $a \in G$ es la función

$$f_a : G \rightarrow G \text{ tal que } f_a(x) = a * x$$

Puede demostrarse fácilmente que toda traslación a izquierda del grupo G es biyectiva.

Análogamente se define la traslación a derecha.

Si $T(G) = \{f : G \to G \,/\, f \text{ es biyectiva}\}$, entonces de acuerdo con el ejemplo 8-3, $(T(G), \circ)$ es un grupo, llamado de las trasformaciones de G.

Toda traslación a izquierda de G es una trasformación de G, es decir

$$a \in G \Rightarrow f_a \in T(G)$$

Si G es finito, entonces el conjunto T (G) es el de permutaciones de G.

*Ejemplo 8-21.*

Sea G un grupo. Entonces la función

$$g: G \to T(G) \text{ tal que } g(a) = f_a \text{ para todo } a \in G,$$

es un morfismo inyectivo de G en T (G).

i ) $g$ es un morfismo pues

$$\forall a\ \forall b\ \forall x \in G : (g(a * b))(x) = f_{a*b}(x) = a * b * x =$$

$$= f_a[f_b(x)] = (f_a \circ f_b)(x)$$

y por definición de funciones iguales resulta

$$g(a * b) = f_a \circ f_b$$

ii ) $g$ es $1 - 1$.

Sea $a \in N(g)$. Entonces $g(a) = f_a = i_G$ por definición de núcleo.

Como

$$a * a = f_a(a) = i_G(a) = a$$

Se tiene

$$a * a = a * e$$

Y cancelando resulta

$$a = e$$

Es decir: $N(g) = \{e\}$ y en consecuencia $g$ es $1 - 1$.

## 8.14. GRUPOS FINITOS

### 8.14.1. Indice de un subgrupo

Sea G un grupo. Por definición, G es finito si y sólo si $c(G) = n$. Orden de un grupo finito es el número cardinal del mismo.

Sea H un subgrupo del grupo finito G. El grupo cociente $\frac{G}{H}$, de las coclases a izquierda de H, es finito y su cardinal se llama índice del subgrupo H en G.

**8.14.2. Teorema** Si H es un subgrupo de orden $k$ del grupo finito G, entonces toda coclase a izquierda de H tiene $k$ elementos.
Hipótesis) $(G, *)$ es grupo finito.
$(H, *)$ es subgrupo de $(G, *)$, de orden $k$.
Tesis) $c(uH) = k$ para todo $u \in G$.
Demostración)
Debemos probar que H y $u$H son coordinables, y para ello definimos

$$f : H \to uH \quad \text{mediante} \quad f(a) = u * a$$

i ) $f$ es la restricción de la traslación a izquierda $f_u : G \to G$ al subconjunto H, y en consecuencia es inyectiva.

ii ) $f$ es sobreyectiva, pues para todo $y \in uH$ existe $x = u' * y$, tal que

$$f(x) = f(u' * y) = u * u' * x = x$$

En consecuencia, $f$ es biyectiva y $c(uH) = c(H) = k$.

**8.14.3. Teorema de Lagrange.** El orden de todo subgrupo de un grupo finito es divisor del orden del grupo.

En efecto, si H es un subgrupo de G y o (H) = $k$, por 8.14.2. el cardinal de toda coclase a izquierda de H es $k$, y como éstas son disjuntas resulta

$$o(G) = m \cdot k = m \cdot o(H)$$

Es decir

$$o(H) \mid o(G).$$

# TRABAJO PRACTICO VIII

*8-22.* Determinar en cada caso si el par (G , $*$) es grupo

a) $G = \left\{ x \,/\, x = 2k + 1 \ \wedge \ k \in \mathbf{Z} \right\}$
$*$ es el producto ordinario

b) $G = \left\{ x \,/\, x = 3k \ \wedge \ k \in \mathbf{Z} \right\}$
$*$ es la adición en Z

c) $G = \left\{ a + b\sqrt{2} \,/\, a \in \mathbf{Q} \ \wedge \ b \in \mathbf{Q} \right\}$
$*$ es el producto habitual

d) $G = \left\{ x \,/\, x = 2^k \ \wedge \ k \in \mathbf{Z} \right\}$
$*$ es el producto

*8-23.* Verificar que los siguientes conjuntos son grupos cíclicos multiplicativos, y determinar sus generadores

i ) $G = \left\{ 1 , -1 , i , -i \right\}$

ii ) $G = \left\{ 1 , z , z^2 \right\}$ siendo $z = -\dfrac{1}{2} + i\,\dfrac{\sqrt{3}}{2}$

*8-24.* En $\mathbf{R}^+$ se define $*$ mediante

$$a * b = 2\,a\,b$$

Verificar que $(\mathbf{R}^+ , *)$ es grupo abeliano.

*8-25.* En el conjunto C de los números complejos se considera $*$ definida por

$$a * b = a + b - i$$

Probar que (C , $*$) es grupo abeliano.

*8-26.* En $\mathbf{R}^{\mathbf{I}} = \left\{ f \,/\, f : [0\,,1] \to \mathbf{R} \right\}$ se define la suma de funciones por medio de

$$(f + g)(x) = f(x) + g(x)$$

Demostrar que $(\mathbf{R}^{\mathbf{I}} , +)$ es grupo abeliano.

*8-27.* Demostrar que $(\mathbf{R}^n , +)$ es grupo abeliano, siendo $\mathbf{R}^n$ el conjunto de todas las $n$-uplas de números reales, y la suma definida por

$$(x_1 , x_2 , \ldots , x_n) + (y_1 , y_2 , \ldots , y_n) = (x_1 + y_1 , x_2 + y_2 , \ldots , x_n + y_n)$$

*8-28.* Formar el conjunto de todas las simetrías y rotaciones del triángulo equilátero

que lo transforman congruentemente, y verificar que dicho conjunto con la composición de funciones es un grupo. Formar la tabla.

*8-29.* Determinar todos los subgrupos en el caso del ejercicio anterior.

*8-30.* Sea $H = \left\{ (x_1, x_2, \ldots, x_n) \in R^n \ / \ x_i = 0 \right\}$. Demostrar que $(H, +)$ es un subgrupo de $(R^n, +)$.

*8-31.* Verificar que $(R^{2\times 2}, +)$ es un grupo abeliano y que $(H, +)$ es un subgrupo, siendo H el conjunto de las matrices reales de dos filas y dos columnas que verifican $A = -A^t$.
Tales matrices se llaman antisimétricas y satisfacen $a_{ij} = -a_{ij} \ \forall i \ \forall j$.

*8-32.* Sean $A = R - \{0\}$ y la función $f : A \to A$ tal que $f(x) = x^2$. Demostrar que $f$ es un morfismo del grupo $(A, .)$ en sí mismo, y determinar su núcleo y su imagen.

*8-33.* Investigar si $f : A \to A$ definida por $f(x) = x^3$ es un morfismo, en el mismo caso del ejercicio anterior.

*8-34.* Demostrar que $f : R^+ \to R$ tal que $f(x) = \log_2 x$ es un isomorfismo de $(R^+, .)$ en $(R, +)$.

*8-35.* Sean $f$ un homomorfismo del grupo G en el grupo G', y H un subgrupo de G'. Demostrar que su preimagen $f^{-1}(H)$ es un subgrupo de G.

*8-36.* Sean $(G, *)$ un grupo con la propiedad siguiente:

$$\forall x \in G : x * x = x$$

Demostrar que G es unitario.

*8-37.* Si $(G, *)$ es un grupo que verifica $x * x = e$ para todo $x \in G$, entonces es conmutativo.

*8-38.* Sean $(G, *)$ un grupo y $a$ un elemento fijo de G. Se define

$$f_a : G \to G \ \text{ mediante } \ f(x) = a^{-1} * x * a$$

Demostrar que $f_a$ es un automorfismo en G. Tal automorfismo, definido por $a \in G$, se llama automorfismo interno.

*8-39.* Demostrar que la composición de dos homomorfismos de grupos es un homomorfismo.

*8-40.* Sea Aut (G) el grupo de los automorfismos del grupo $(G, *)$, con la composición de funciones. Demostrar que la función

$$F : G \to \text{Aut}(G) \ \text{ definida por } \ F(a) = f_a$$

es un morfismo.

*8-41.* Sea $(G, *)$ un grupo. En G se define la operación $\circ$ mediante

$$a \circ b = b * a$$

Demostrar que $(G, \circ)$ es un grupo y que ambos se identifican si y sólo si $*$ es conmutativa.

*8-42.* Con relación a los grupos del ejercicio anterior, demostrar que la función
$$f : (G , *) \to (G , \circ) \text{ definida por } f(x) = x'$$
es un isomorfismo.

*8-43.* En $Q^2$ se considera $*$ definida por
$$(a , b) * (c , d) = (ac , bc + d)$$
Determinar si $Q^2$ tiene estructura de grupo con $*$.

*8-44.* Sean S y T dos subgrupos del grupo aditivo (G , +). Se define
$$S + T = \left\{ x + y \ / \ x \in S \ \wedge \ y \in T \right\}$$
Demostrar que S + T es un subgrupo de G.

*8-45.* Demostrar que en todo grupo el único elemento idempotente es el neutro.

*8-46.* Demostrar que el semigrupo (X , $*$) es un grupo si y sólo si las ecuaciones $x * a = b$ y $a * x = b$ son resolubles en X.

*8-47.* Sean los grupos (G , $*$) y (G' , $*'$) y $f : G \to G'$ un homomorfismo. Demostrar que $f$ es un epimorfismo si y sólo si $I(f) = G'$.

*8-48.* Sean los grupos (**Z** , +) y (G , $*$) y la función $f : \mathbf{Z} \to G$ tal que $f(n) = a^n$ con $a \in G$. Demostrar que $f$ es un morfismo y que su imagen es el subgrupo cíclico de G, generado por $a$.

*8-49.* Sean los grupos ($\mathbf{R}^3$ , +) y ($\mathbf{R}^2$ , +). Probar que $f : \mathbf{R}^3 \to \mathbf{R}^2$ definida por $f(x_1, x_2, x_3) = (x_1 - x_3 , x_2 - x_3)$ es un homomorfismo. Determinar su núcleo y su imagen.

*8-50.* El subgrupo H de G es normal, si y sólo si $u$H = H$u$.

*8-51.* Sean los grupos ($G_3$ , .) y ($G_4$ , .). Demostrar que la función $f : G_3 \to G_4$ definida por $f(z) = z^{3/4}$ es un homomorfismo, y determinar N ($f$) e I ($f$).

*8-52.* Demostrar que el subgrupo H de G es normal si y sólo si la imagen de H es igual a H para cada automorfismo interior de G. Tal subgrupo se llama invariante.

Capítulo 9

# ESTRUCTURAS DE ANILLO Y DE CUERPO. ENTEROS Y RACIONALES

## 9.1. INTRODUCCION

Con el agregado de una ley de composición interna sujeta a ciertas condiciones, se enriquece la estructura de grupo abeliano y la terna así obtenida constituye otro sistema axiomático. Se definen aquí la estructura de anillo y el caso particular de cuerpo. Lo mismo que en el caso de la estructura de grupo, se estudian sus propiedades básicas y se introduce el concepto de ideal. Después de tratar la factorización en los dominios de integridad principales, se introducen el anillo de los enteros y el cuerpo de los racionales.

## 9.2. ESTRUCTURA DE ANILLO

Sean un conjunto no vacío A, y dos funciones: $*$ y $\bullet$

***Definición***

La terna $(A , * , \bullet)$ es un anillo si y sólo si

1. El conjunto con la primera ley es un grupo abeliano.
2. El conjunto con la segunda ley es un semigrupo.
3. La segunda ley es doblemente distributiva respecto de la primera.

Reformulamos la definición teniendo en cuenta que las dos leyes de composición se llaman aditiva y multiplicativa, y que se las suele denotar con + y . , respectivamente.

***Definición***

La terna $(A , + , .)$ es un anillo si y sólo si

1. $(A, +)$ es un grupo abeliano.
2. $(A , .)$ es un semigrupo.
3. El producto es distributivo a izquierda y derecha respecto de la suma.

Estas condiciones se traducen en los siguientes axiomas:

$A_1$: La adición es ley de composición interna en A.

$$\forall a\ \forall b : a \in A\ \wedge\ b \in A \Rightarrow a + b \in A$$

$A_2$ : La adición es asociativa en A.

$$\forall a\ \forall b\ \forall c \in A : (a + b) + c = a + (b + c)$$

$A_3$ : Existe neutro en A, que denotamos con 0, respecto de la adición

$$\exists\, 0 \in A \,/\, \forall a \in A : a + 0 = 0 + a = a$$

$A_4$ : Todo elemento de A admite inverso aditivo u opuesto.

$$\forall a \in A\,,\ \exists -a \in A \,/\, a + (-a) = (-a) + a = 0$$

$A_5$ : La adición es conmutativa

$$\forall a\ \forall b \in A : a + b = b + a$$

$A_6$ : El producto es ley de composición interna en A.

$$\forall a\ \forall b : a \in A\ \wedge\ b \in A \Rightarrow a\,.\,b \in A$$

$A_7$ : El producto es asociativo en A.

$$\forall a\ \forall b\ \forall c \in A : (a\,.\,b)\,.\,c = a\,.\,(b\,.\,c)$$

$A_8$ : El producto es doblemente distributivo respecto de la suma.

$$\forall a\ \forall b\ \forall c \in A : \begin{cases} a\,.\,(b + c) = a\,.\,b + a\,.\,c \\ (b + c)\,.\,a = b\,.\,a + c\,.\,a \end{cases}$$

Si, además, ocurre que la segunda ley de composición es conmutativa diremos que el anillo (A , + , .) es conmutativo. Si existe elemento neutro o identidad respecto del producto, que denotamos con 1, entonces se llamará anillo con identidad o con unidad. Un anillo con identidad cuyos elementos no nulos son inversibles se llama anillo de división.

*Ejemplo 9-1.*

Clasificamos las siguientes ternas

i ) (**N** , + , .) no es anillo, pues no existe neutro para la adición.

ii ) ($\mathbf{N_0}$ , + , .) no es anillo, porque los elementos no nulos de $\mathbf{N_0}$ carecen de inverso aditivo.

iii) (**Z** , + , .) es anillo conmutativo y con unidad.

iv) ($\mathbf{R}^I$ , + , .) es el anillo conmutativo y con unidad de las funciones reales definidas en $I = [0\,,1]$ con la suma y el producto de funciones, llamadas leyes de composición punto a punto, definidas en los ejercicios 5-31 y 5-36.

## 9.3. PROPIEDADES DE LOS ANILLOS

**9.3.1.** El producto de cualquier elemento de un anillo por el neutro para la primera ley es igual a éste.

Hipótesis) $(A, +, .)$ es anillo.

Tesis) $a \,.\, 0 = 0 \,.\, a = 0$

Demostración)

Cualquiera que sea $x \in A$, por $A_3$ se verifica

$$x + 0 = x$$

Premultiplicando por $a$

$$a \,.\, (x + 0) = a \,.\, x$$

Por la distributividad

$$a \,.\, x + a \,.\, 0 = a \,.\, x$$

En virtud de $A_3$

$$a \,.\, x + a \,.\, 0 = a \,.\, x + 0$$

Por ley cancelativa en el grupo $(A, +)$

$$a \,.\, 0 = 0$$

Análogamente se prueba que $0 \,.\, a = 0$.

Esta propiedad suele enunciarse así: en todo anillo, el producto por 0 es 0.

**9.3.2.** En todo anillo, el producto del opuesto de un elemento, por otro, es igual al opuesto de su producto.

Por distributividad, $A_4$ y producto por 0, se tiene

$$(-a) \,.\, b + a \,.\, b = (-a + a) \,.\, b = 0 \,.\, b = 0$$

Es decir

$$(-a) \,.\, b + a \,.\, b = 0$$

Entonces

$$(-a) \,.\, b = -(a \,.\, b)$$

De manera similar se prueba que $a \,.\, (-b) = -(a \,.\, b)$.

**9.3.3.** En todo anillo, el producto de los opuestos de dos elementos es igual al producto de los mismos.

Aplicando reiteradamente la propiedad 9.3.2., y por opuesto del opuesto, resulta

$$(-a) \,.\, (-b) = -[a \,.\, (-b)] = -[-(a \,.\, b)] = a \,.\, b$$

9.3.4. En todo anillo vale la distributividad del producto respecto de la diferencia.
Se trata de probar que $(a-b).c=a.c-b.c$
Por definición, se sabe que $a-b=a+(-b)$. Entonces, aplicando $A_8$ y 9.3.2.

$$(a-b).c=[a+(-b)].c=a.c+(-b).c=a.c+[-(b.c)]=a.c-b.c$$

## 9.4. ANILLO SIN DIVISORES DE CERO

### 9.4.1. Concepto

En el ejemplo 5-15 hemos analizado las leyes de composición interna, llamadas suma y producto de clases, inducidas en el conjunto cociente de **Z** por la relación de congruencia módulo $n=3$. De acuerdo con 9.2 resulta $(\mathbf{Z}_3, +, .)$ el anillo conmutativo y con unidad de las clases de restos módulo 3. En los ejemplos 5-15 y 5-16 hemos confeccionado las tablas de la adición y multiplicación en $\mathbf{Z}_3$ y $\mathbf{Z}_4$. En el primer caso hemos observado que elementos no nulos dan producto no nulo; pero en el segundo caso ocurre que hay elementos no nulos cuyo producto es nulo. En $(\mathbf{Z}_3, +, .)$ elementos no nulos dan producto no nulo, y se dice que no existen divisores de cero. En $(\mathbf{Z}_4, +, .)$, en cambio, hay divisores de cero.

***Definición***

El anillo (A , + , .) no tiene divisores de cero si y sólo si elementos no nulos dan producto no nulo.

En símbolos

$$(A, +, .) \text{ carece de divisores de cero} \Leftrightarrow \forall x\, \forall y : x \neq 0 \;\wedge\; y \neq 0 \Rightarrow x.y \neq 0$$

Equivalentemente, por medio de la implicación contrarrecíproca se tiene

$$(A, +, .) \text{ carece de divisores de cero} \Leftrightarrow \forall x\, \forall y : x.y = 0 \Rightarrow x = 0 \;\vee\; y = 0$$

Esto significa que, para demostrar que en un anillo no existen divisores de cero, es suficiente probar que si el producto de dos elementos cualesquiera es cero, entonces alguno de los factores es cero.

Negando el antecedente y el consecuente del bicondicional que expresa simbólicamente la definición, resulta

$$(A, +, .) \text{ tiene divisores de cero} \Leftrightarrow \exists x\, \exists y \;/\; x \neq 0 \;\wedge\; y \neq 0 \;\wedge\; x.y = 0$$

***Definición***

El anillo (A , + , .) tiene divisores de cero si y sólo si existen elementos no nulos que dan producto nulo.

9.4.2. **Propiedad.** El anillo $(\mathbf{Z}_n, +, .)$ no tiene divisores de cero si y sólo si $n$ es primo.
Por definición, el número natural $n>1$ es primo si y sólo si los únicos divisores

naturales que admite son 1 y $n$. Decimos que $n > 1$ es compuesto si y sólo si $n = x \,.\, y$, siendo $1 < x < n$ y $1 < y < n$.

I) Si $(\mathbf{Z}_n , + , .)$ no tiene divisores de cero, entonces $n$ es primo.

Suponemos que $n$ es compuesto, es decir

$$n = x \,.\, y \quad \text{donde} \quad 1 < x < n \quad \text{y} \quad 1 < y < n \qquad (1)$$

Si $f : \mathbf{Z} \to \mathbf{Z}_n$ es la aplicación canónica, se tiene

$$f\,(n) = f\,(x \,.\, y)$$

Como $f$ es un morfismo respecto del producto

$$f\,(n) = f(x) \,.\, f(y)$$

De acuerdo con (1)

$$f(x) = \overline{x} \quad \text{y} \quad f(y) = \overline{y}\,.$$

Además, como $n \sim 0$, por definición de aplicación canónica e imagen del neutro por un homorfismo, es

$$f\,(n) = f(0) = \overline{0}$$

Sustituyendo en la igualdad anterior resulta

$$\overline{0} = \overline{x} \,.\, \overline{y} \ \wedge \ \overline{x} \neq \overline{0} \ \wedge \ \overline{y} \neq \overline{0}$$

lo que nos dice que en $\mathbf{Z}_n$ hay divisores de cero, contra la hipótesis.

II) Si $n$ es primo, entonces $(\mathbf{Z}_n , + , .)$ no tiene divisores de cero.

Sean $\overline{x}$ y $\overline{y}$ en $\mathbf{Z}_n$ tales que $\overline{x} \,.\, \overline{y} = \overline{0}$. Se trata de probar que $\overline{x} = \overline{0} \ \vee \ \overline{y} = \overline{0}$. Por definición de aplicación canónica, la igualdad anterior puede escribirse

$$f(x) \,.\, f(y) = f(0)$$

Por ser $f$ un morfismo

$$f\,(x \,.\, y) = f(0)$$

Y por definición de función canónica

$$x \,.\, y \sim 0$$

Por definición de congruencia módulo $n$

$$n \mid x \,.\, y$$

Anticipamos el uso de una propiedad que demostraremos en 9.7.7., a saber: si un número primo es divisor de un producto, entonces es divisor de alguno de los factores. En consecuencia

$$n \mid x \ \vee \ n \mid y$$

Es decir

$$x \sim 0 \ \vee \ y \sim 0$$

En consecuencia

$$\bar{x} = \bar{0} \ \vee \ \bar{y} = \bar{0}$$

### 9.4.3. Ley cancelativa del producto

En el anillo $(\mathbf{Z}, +, .)$ se verifica la ley cancelativa del producto para todo elemento no nulo

$$a \,.\, b = a \,.\, c \ \wedge \ a \neq 0 \Rightarrow b = c$$

En cambio en $(\mathbf{Z}_{12}, +, .)$ es falsa la proposición

$$\bar{3} \,.\, \bar{4} = \bar{3} \,.\, \bar{8} \Rightarrow \bar{4} = \bar{8}$$

por ser V el antecedente y F el consecuente. Es decir, en $\mathbf{Z}_{12}$ no es válida la ley cancelativa del producto para todo elemento no nulo del anillo. La no existencia de divisores de cero es condición necesaria y suficiente para la validez de la ley cancelativa del producto.

**Propiedad**. Un anillo no tiene divisores de cero si y sólo si vale la ley cancelativa del producto para todo elemento no nulo del mismo.

I) Hipótesis) (A , + , .) carece de divisores de cero.

$$x \,.\, z = y \,.\, z \ \wedge \ z \neq 0$$

Tesis) $x = y$

Demostración)

Por hipótesis es

$$x \,.\, z = y \,.\, z.$$

Por trasposición en (A , +)

$$x \,.\, z - y \,.\, z = 0$$

Por distributividad

$$(x - y) \,.\, z = 0$$

Como no existen divisores de cero y $z \neq 0$ resulta

$$x - y = 0$$

Es decir

$$x = y$$

II) Hipótesis) (A , + , .) es tal que $a \,.\, c = b \,.\, c \ \wedge \ c \neq 0 \Rightarrow a = b$

$$x \,.\, y = 0$$

Tesis) $x = 0 \vee y = 0$

Demostración)

Suponemos que $y \neq 0$. Debe ser necesariamente $x = 0$.

Por $A_3$, cualquiera que sea $z \in A$, se verifica

$$z \cdot y = z \cdot y + 0$$

Como por hipótesis $x \cdot y = 0$, se tiene

$$z \cdot y = z \cdot y + x \cdot y$$

Por distributividad

$$z \cdot y = (z + x) \cdot y$$

Por ley cancelativa, ya que $y \neq 0$, resulta

$$z = z + x$$

Es decir

$$x = 0$$

***Ejemplo 9-2.***

En el conjunto $\mathbf{R}^{n \times n}$, de todas las matrices reales de $n$ filas y $n$ columnas, se define la multiplicación por medio de la siguiente regla: si A y B son dos matrices $n \times n$, entonces la matriz producto $C = A \cdot B$ es tal que el elemento genérico $c_{ij}$ es igual a la suma de productos de los elementos de la fila $i$ de A, por los correspondientes elementos de la columna $j$ de B, es decir

$$c_{ij} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + \ldots + a_{in} \cdot b_{nj} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$$

Por ejemplo, si $A = \begin{bmatrix} -1 & 2 & 0 \\ 3 & 0 & 1 \\ 0 & -1 & 1 \end{bmatrix}$ y $B = \begin{bmatrix} 2 & 1 & -1 \\ 0 & 4 & 3 \\ -1 & -2 & -3 \end{bmatrix}$, entonces la matriz producto $C = A \cdot B$ pertenece a $\mathbf{R}^{3 \times 3}$, y es tal que

$$c_{11} = (-1) \cdot 2 + 2 \cdot 0 + 0 \cdot (-1) = -2$$

$$c_{12} = (-1) \cdot 1 + 2 \cdot 4 + 0 \cdot (-2) = 7 \quad \text{, etcétera. Entonces}$$

$$C = A \cdot B = \begin{bmatrix} -1 & 2 & 0 \\ 3 & 0 & 1 \\ 0 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 & -1 \\ 0 & 4 & 3 \\ -1 & -2 & -3 \end{bmatrix} = \begin{bmatrix} -2 & 7 & 7 \\ 5 & 1 & -6 \\ -1 & -6 & -6 \end{bmatrix}$$

Al desarrollar el trabajo práctico que se propone al término del capítulo, el lector podrá comprobar que el producto de matrices es asociativo, no conmutativo, con neutro, y distributivo a izquierda y derecha respecto de la suma.

El elemento neutro es la matriz identidad $I \in \mathbf{R}^{n \times n}$, tal que

$$a_{ij} = 1 \quad \text{si} \quad i = j$$
$$a_{ij} = 0 \quad \text{si} \quad i \neq j$$

Es decir, está formada por unos en la diagonal y por ceros fuera de ésta.

De acuerdo con lo expuesto, y teniendo en cuenta el ejemplo 5-8, la terna $(\mathbf{R}^{n \times n}, +, .)$ satisface

$A_1 : A \in \mathbf{R}^{n \times n} \ \wedge \ B \in \mathbf{R}^{n \times n} \Rightarrow A + B \in \mathbf{R}^{n \times n}$

$A_2 : (A + B) + C = A + (B + C)$

$A_3 : \exists\, N \in \mathbf{R}^{n \times n} \,/\, \forall\, A \in \mathbf{R}^{n \times n} : A + N = N + A = A$

$A_4 : \forall\, A \in \mathbf{R}^{n \times n},\ \exists - A \in \mathbf{R}^{n \times n} \,/\, A + (-A) = (-A) + A = N$

$A_5 : A + B = B + A$

$A_6 : A \in \mathbf{R}^{n \times n} \ \wedge \ B \in \mathbf{R}^{n \times n} \Rightarrow A \,.\, B \in \mathbf{R}^{n \times n}$

$A_7 : (A \,.\, B) \,.\, C = A \,.\, (B \,.\, C)$

$A_8 : \exists\, I \in \mathbf{R}^{n \times n} \,/\, \forall\, A \in \mathbf{R}^{n \times n} : A \,.\, I = I \,.\, A = A$

$A_9 : A \,.\, (B + C) = A \,.\, B + A \,.\, C \ \wedge \ (B + C) \,.\, A = B \,.\, A + C \,.\, A$

Se trata del anillo no conmutativo, con identidad, de las matrices cuadradas $n \times n$.

Podemos verificar la existencia de divisores de cero en el caso particular $(\mathbf{R}^{2 \times 2}, +, .)$, mostrando que matrices no nulas pueden dar producto nulo. En efecto

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix} \neq N \quad \text{y} \quad B = \begin{bmatrix} -1 & 0 \\ 1 & 0 \end{bmatrix} \neq N, \quad \text{y sin embargo}$$

$$A \,.\, B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = N$$

*Ejemplo 9-3.*

La terna $(P(U), \Delta, \cap)$ es un anillo conmutativo, con identidad y con divisores de cero. En efecto

1. $(P(U), \Delta)$ es grupo abeliano, como está justificado en 2.11.2.
2. $(P(U), \cap)$ es un semigrupo conmutativo, con identidad.
3. La intersección es distributiva respecto de la diferencia simétrica.

$$A \cap (B \Delta C) = (B \Delta C) \cap A = (B \cap A) \wedge (C \cap A)$$

La demostración figura en el ejemplo 2-28.

4. Existen divisores de cero, pues si A y B son disjuntos y no vacíos se cumple

$$A \neq \phi \ \wedge \ B \neq \phi \ \wedge \ A \cap B = \phi$$

## 9.5. DOMINIO DE INTEGRIDAD

Todo anillo conmutativo, con unidad y sin divisores de cero, se llama dominio de integridad.

Las ternas $(\mathbf{Z}, +, .)$, $(\mathbf{R}, +, .)$ y $(\mathbf{Z}_3, +, .)$ son dominios de integridad. Si P denota el conjunto de los enteros pares, entonces $(P, +, .)$ es anillo conmutativo, sin divisores de cero y sin elemento unidad; en consecuencia no es dominio de integridad.

## 9.6. SUBANILLOS E IDEALES

### 9.6.1. Concepto de subanillo

Sea $(A, +, .)$ un anillo. Un subanillo de $(A, +, .)$ es una parte no vacía de A que tiene estructura de anillo con las mismas leyes de composición.

***Definición***

El subconjunto no vacío $S \subset A$ es un subanillo de $(A, +, .)$ si y sólo si $(S, +)$ es subgrupo de $(A, +)$, y además S es cerrado para el producto.

Resulta obvio que una parte no vacía $S \subset A$ es un subanillo de $(A, +, .)$ si y sólo si para todo par de elementos $a \in A$ y $b \in A$ se verifica $a - b \in A$ y $a \,.\, b \in A$.

*Ejemplo 9-4.*

Sea $a \in \mathbf{Z}$. Entonces el conjunto de todos los múltiplos enteros de $a$

$$S = \left\{ k \,.\, a \,/\, k \in \mathbf{Z} \right\}$$

es un subanillo de $(\mathbf{Z}, +, .)$.

En efecto, si $x \in S \wedge y \in S$, entonces $x = k \,.\, a \wedge y = k' \,.\, a$.

Luego

$$x - y = k \,.\, a - k' \,.\, a = (k - k') \,.\, a = k'' \,.\, a$$

Es decir

$$x - y \in S$$

Por otra parte

$$x \in S \wedge y \in S \Rightarrow x = k \,.\, a \wedge y = k' \,.\, a \Rightarrow$$
$$\Rightarrow x \,.\, y = (k \,.\, a \,.\, k') \,.\, a \Rightarrow x \,.\, y = k'' \,.\, a \Rightarrow x \,.\, y \in S$$

### 9.6.2. Concepto de ideal

Sea $(I, +, .)$ un subanillo de $(A, +, .)$.

***Definición***

El subanillo I de A es un ideal a izquierda de A si y sólo si

$$x \in A \;\wedge\; a \in I \Rightarrow x \,.\, a \in I$$

El subanillo I de A es un ideal a derecha de A si y sólo si

$$a \in I \;\wedge\; x \in A \Rightarrow a \,.\, x \in I$$

***Definición***

El subanillo I de A es un ideal de A si y sólo si es un ideal a izquierda y a derecha de A.

En el caso de anillo conmutativo no es preciso distinguir entre ideales a izquierda o a derecha.

Las condiciones que se imponen al subconjunto $I \subset A$, para que sea un ideal, son las siguientes

i ) $I \neq \phi$

ii ) $a \in I \;\wedge\; b \in I \Rightarrow a - b \in I$

iii) $a \in I \;\wedge\; b \in I \Rightarrow a \,.\, b \in I$

iv) $a \in I \;\wedge\; x \in A \Rightarrow a \,.\, x \in I \;\wedge\; x \,.\, a \in I$

***Ejemplo 9-5.***

El subanillo S de todos los múltiplos del entero $a$ es un ideal de **Z**.
En cambio, **Z** no es un ideal de **R**.

Todo anillo (A , + , . ) admite dos ideales: el mismo A y $\{0\}$, y son llamados ideales triviales. Todo otro ideal, si existe, se llama ideal propio no trivial.

### 9.6.3. Ideal generado por un subconjunto de un anillo

Sea $S = \{x_1, x_2, \ldots, x_n\}$ un subconjunto no vacío del anillo conmutativo A. Todo elemento de la forma

$$\sum_{i=1}^{n} a_i \,.\, x_i \quad \text{con} \quad a_i \in A$$

se llama combinación lineal de los elementos de S, con coeficientes en A.

Consideremos ahora el conjunto de todas las combinaciones lineales de los elementos de S, que denotamos por

$$\overline{S} = \left\{ \sum_{i=1}^{n} a_i \,.\, x_i \,/\, a_i \in A \;\wedge\; x_i \in S \right\}$$

El conjunto $\overline{S} \subset A$ satisface las siguientes condiciones:

i) $\overline{S} \neq \phi$ pues $0 = 0 . x_1 + 0 . x_2 + \ldots + 0 . x_n \in \overline{S}$

ii) $x \in \overline{S} \wedge y \in \overline{S} \Rightarrow x - y \in \overline{S}$

iii) $x \in \overline{S} \wedge y \in \overline{S} \Rightarrow x . y \in \overline{S}$

iv) $x \in \overline{S} \wedge a \in A \Rightarrow a . x \in \overline{S} \wedge x . a \in \overline{S}$

Es decir: $(\overline{S}, +, .)$ es un ideal de A. Este ideal se dice generado por la familia S.

En particular, el ideal generado por un único elemento $x \in A$ se llama ideal principal. Si ocurre que todo ideal de A es principal, entonces el mismo A se llama anillo principal. Este es el caso de los enteros, que está generado por $x = 1$.

El lector puede verificar las condiciones iii) y iv). A manera de ejemplo comprobamos ii)

$$x \in \overline{S} \wedge y \in \overline{S} \Rightarrow x = \sum_{i=1}^{n} a_i . x_i \wedge y = \sum_{i=1}^{n} b_i . x_i \Rightarrow$$

$$\Rightarrow x - y = \sum_{i=1}^{n} (a_i . x_i - b_i . x_i) \Rightarrow$$

$$\Rightarrow x - y = \sum_{i=1}^{n} (a_i - b_i) . x_i \Rightarrow x - y = \sum_{i=1}^{n} c_i x_i \Rightarrow$$

$$\Rightarrow x - y \in \overline{S}$$

## 9.7. FACTORIZACION EN UN ANILLO

Sea $(A, +, .)$ un dominio de integridad principal. En este caso, todo ideal de A está generado por un único elemento.

### 9.7.1. Máximo común divisor

En A definimos la relación de divisor mediante

$$x \mid y \Leftrightarrow \exists\, z \in A \,/\, y = x . z$$

Si $d$ es tal que $d \mid a$ y $d \mid b$, entonces se dice que $d$ es un divisor común de $a$ y de $b$, o bien que $a$ y $b$ son múltiplos de $d$.

***Definición***

El elemento $d \in A$ es un máximo común divisor de $a$ y $b$ si y sólo si $d$ es divisor de $a$ y $b$, y además múltiplo de todo divisor común a ellos.

Es decir

$$d \text{ es un M.C.D. de } a \text{ y } b \Leftrightarrow \begin{cases} d \mid a \wedge d \mid b \\ d' \mid a \wedge d' \mid b \Rightarrow d' \mid d \end{cases}$$

En $\mathbf{Z}$, tanto 2 como $-2$, son un M.C.D. de 4 y 6.

**9.7.2. Propiedad.** Todo elemento inversible de A es divisor de todo elemento del mismo.

En efecto, sea $a \in A$ un elemento inversible.

Entonces

$$\forall x \in A : x = x \,.\, 1 = x\,(a^{-1} \,.\, a) =$$
$$= (x \,.\, a^{-1}) \,.\, a$$

y por definición de divisor resulta

$$a \mid x$$

**9.7.3. Propiedad.** Todo M.C.D. de los elementos $a$ y $b$ de A es una combinación lineal de los mismos con coeficientes en A.

Demostración)

Sea I el ideal de A generado por los elementos $a$ y $b$. Como todo ideal de A es principal, ocurre que I está generado por un único elemento $d$. Por otra parte, como

$$a = 1 \,.\, a + 0 \,.\, b \;\wedge\; b = 0 \,.\, a + 1 \,.\, b$$

se tiene $a \in I \;\wedge\; b \in I$. En consecuencia, existen $p$ y $q$ en A, tales que $a = p \,.\, d$ y $b = q \,.\, d$, es decir, $d$ es un divisor común de $a$ y $b$.

Además, como $d \in I$, existen $s$ y $t$ en A, tales que

$$d = s \,.\, a + t \,.\, b$$

Sea ahora $d'$ un divisor común de $a$ y $b$; entonces $a = x \,.\, d'$ y $b = y \,.\, d'$.

Sustituyendo se tiene

$$d = s \,.\, x \,.\, d' + t \,.\, y \,.\, d' = (s \,.\, x + t \,.\, y) \,.\, d'$$

o sea, $d' \mid d$. Hemos probado que $d = s \,.\, a + t \,.\, b$ es un M.C.D. de $a$ y $b$.

### 9.7.4. Elementos coprimos

En **Z**, los enteros 2 y 3 admiten a $-1$ y a 1 como divisores comunes. Estos son los únicos elementos inversibles en **Z**, y se dice que 2 y 3 son coprimos o primos entre sí.

***Definición***

Dos elementos $a$ y $b$ de A son coprimos si y sólo si todo común divisor de $a$ y $b$ es inversible.

**9.7.5. Propiedad.** Si dos elementos $a$ y $b$ de A son coprimos, entonces existen $s$ y $t$ en A, tales que $1 = s \,.\, a + t \,.\, b$.

Demostración)

La unidad de A verifica $1 \mid a$ y $1 \mid b$; es decir, 1 es un divisor común de $a$ y $b$. Sea ahora $d$ un divisor común de $a$ y $b$. Por ser éstos coprimos, $d$ es inversible y

por lo tanto es divisor de 1, de acuerdo con 9.7.2. Esto prueba que 1 es un M.C.D. de $a$ y $b$, y por 9.7.3., existen $s$ y $t$ en A, tales que

$$1 = s \,.\, a + t \,.\, b$$

**9.7.6. Elementos primos o irreducibles**

En **Z**, el entero 3 es no inversible y admite únicamente las descomposiciones

$$3 = 3 \,.\, 1 \quad \text{y} \quad 3 = (-3) \,.\, (-1)$$

donde 1 y $-1$ son inversibles. Se dice que 3 es primo o irreducible.

***Definición***

El elemento no inversible $a \in A$ es primo o irreducible si y sólo si toda descomposición $a = x \,.\, y$ es tal que alguno de los factores es inversible.

**9.7.7. Propiedad.** Si un elemento primo es divisor de un producto, entonces es divisor de alguno de los factores.
Hipotesis) $a$ es primo y $a \mid b \,.\, c$
Tesis) $a \mid b \vee a \mid c$
Demostración)

Si $a \mid b$, nada hay que probar, porque la disyunción de la tesis es verdadera.

Consideremos el caso en que $a \mid b$ es F. Como $a$ es primo, se tiene que $a$ y $b$ son coprimos, y por 9.7.5. es

$$1 = s \,.\, a + t \,.\, b$$

Multiplicando por $c$

$$1 \,.\, c = s \,.\, a \,.\, c + t \,.\, b \,.\, c$$

Es decir

$$c = s \,.\, a \,.\, c + t \,.\, a \,.\, x \quad \text{ya que} \quad a \mid b \,.\, c \Rightarrow b \,.\, c = a \,.\, x$$

Por distributividad

$$c = (s \,.\, c + t \,.\, x) \,.\, a$$

Luego

$$a \mid c$$

## 9.8. ANILLO ORDENADO

**9.8.1. Concepto**

El anillo (A , + , .) está ordenado por la relación de orden total que indicamos con

el símbolo $<$ si y sólo si dicha relación es compatible con la adición y multiplicación en A, en el sentido siguiente:

i ) $x<y \Rightarrow x+z<y+z$

ii ) $0<x \ \wedge \ 0<y \Rightarrow 0<xy$

Que el orden es total o lineal significa

$$x \in A \Rightarrow x<0 \ \vee \ 0<x \ \vee \ x=0$$

Si el anillo no es trivial, es decir, si no se reduce al único elemento 0, entonces los elementos $x$ que satisfacen la condición $0<x$ se llaman positivos y pertenecen al subconjunto

$$A^{+}=\left\{x \in A \,/\, 0<x\right\}$$

Los opuestos de los elementos positivos se llaman negativos y definen al subconjunto

$$A^{-}=\left\{x \in A \,/ -x \in A^{+}\right\}=\left\{x \in A \,/\, 0<-x\right\}$$

Queda caracterizada así una partición de A en los subconjuntos $A^{+}$, $A^{-}$ y $\left\{0\right\}$, y en consecuencia

$$x \in A \Rightarrow x \in A^{+} \ \vee \ x \in A^{-} \ \vee \ x=0$$

**9.8.2. Propiedades**. Sea (A , + , .) un anillo ordenado por la relación $<$.

I) El producto de dos elementos positivos es positivo.

$$x \in A^{+} \ \wedge \ y \in A^{+} \Rightarrow 0<x \ \wedge \ 0<y \Rightarrow$$
$$\Rightarrow 0<x\,y \Rightarrow x\,y \in A^{+}$$

Por definición de $A^{+}$ y ii ).

En consecuencia, $A^{+}$ es cerrado para el producto.

II) El producto de dos elementos, uno positivo y el otro negativo, es negativo.

$$x \in A^{+} \ \wedge \ y \in A^{-} \Rightarrow 0<x \ \wedge \ 0<-y \Rightarrow$$
$$\Rightarrow 0<x\,(-y) \Rightarrow 0<-(x\,y) \Rightarrow x\,y \in A^{-}$$

Por las definiciones de $A^{+}$ y de $A^{-}$, ii ), 9.3.2., y por definición de $A^{-}$

III) El producto de dos elementos negativos es positivo.

$$x \in A^{-} \ \wedge \ y \in A^{-} \Rightarrow -x \in A^{+} \ \wedge \ -y \in A^{+} \Rightarrow$$
$$\Rightarrow (-x)\,(-y) \in A^{+} \Rightarrow x\,y \in A^{+}$$

Por definición de $A^{-}$, III) y 9.3.3.

IV) $x<y \Leftrightarrow y-x \in A^{+}$

En efecto

$$x<y \Leftrightarrow x+(-x)<y+(-x) \Leftrightarrow 0<y-x$$

V) $x \leq y \ \wedge \ z \in A^+ \Rightarrow xz < yz$

Pues

$$x<y \ \wedge \ z \in A^+ \Rightarrow 0<y-x \ \wedge \ 0<z \Rightarrow$$
$$\Rightarrow 0<(y-x)z \Rightarrow 0<yz-xz \Rightarrow xz<yz$$

VI) $x<y \ \wedge \ z \in A^- \Rightarrow yz<xz$

$$x<y \ \wedge \ z \in A^- \Rightarrow 0<y-x \ \wedge \ -z \in A^+ \Rightarrow$$
$$\Rightarrow 0<(y-x)(-z) \Rightarrow 0<-yz+xz \Rightarrow yz<xz$$

*Nota*

La relación inversa se denota por $>$, y se define mediante

$$x>y \Leftrightarrow y<x$$

y ambas caracterizan un orden estricto en A.

Un orden amplio y total en A se define mediante

$$x \leqslant y \Leftrightarrow x<y \ \vee \ x=y$$

## 9.9. ESTRUCTURA DE CUERPO

### 9.9.1. Concepto de cuerpo

Un anillo con unidad cuyos elementos no nulos son inversibles, se llama anillo de división. Todo anillo de división conmutativo es un cuerpo.

***Definición***

La terna (K , + , .) es un cuerpo si y sólo si es un anillo conmutativo, con unidad, cuyos elementos no nulos admiten inverso multiplicativo.

Los axiomas que caracterizan la estructura de cuerpo son

1. (K , +) es grupo abeliano.
2. $(K-\{0\}, .)$ es grupo abeliano.
3. El producto es distributivo respecto de la suma.

***Ejemplo 9-6.***

La terna (Z , + , .) no es cuerpo, pues los únicos elementos no nulos que admiten inverso multiplicativo son $-1$ y 1.

En cambio (**Q** , + , .) , (**R** , + , .) , (**C** , + , .) , ($\mathbf{Z}_n$ , + , .), con $n$ primo, son cuerpos.

### 9.9.2. Propiedades de los cuerpos

Sea (K , + , .) un cuerpo.

I) Los cuerpos no admiten divisores de cero.

Sean $x \in K \wedge y \in K$ tales que $xy = 0$ (1).

Si $x = 0$, nada hay que demostrar porque la proposición $x = 0 \vee y = 0$ es V.

Consideremos el caso $x \neq 0$. Por definición de cuerpo existe $x^{-1}$.

Multiplicando (1) por $x^{-1}$

$$x^{-1}(xy) = x^{-1} \cdot 0$$

Por asociatividad y producto por 0 en el anillo, se tiene

$$1\, y = 0 \text{ , es decir: } y = 0$$

II) En todo cuerpo vale la ley cancelativa del producto para todo elemento no nulo del mismo.

Es una consecuencia de I y de 9.4.3.

III) Si $b \neq 0$, entonces la ecuación $bx = a$ admite solución única en K.

Sea $bx = a$ con $b \neq 0$.

Multplicando por $b^{-1}$

$$b^{-1}(bx) = b^{-1}\, a$$

Por asociatividad y conmutatividad resulta

$$(b^{-1}\, b)\, x = ab^{-1}$$

Es decir

$$1\, x = ab^{-1}$$

Entonces

$$x = ab^{-1}$$

es la solución única de la ecuación propuesta. En efecto, sea $y$ otra solución; esto significa que

$$by = a \text{ , y como } bx = a \text{ se tiene}$$

$$by - bx = 0 \Rightarrow b(y - x) = 0$$

y como $b \neq 0$ resulta $y - x = 0$, es decir, $y = x$.

*Nota*

El producto de un elemento de K por el inverso multiplicativo de otro no nulo se denota con el símbolo

$$ab^{-1} = \frac{a}{b} \text{ ,}$$

y suele llamarse cociente entre $a$ y $b$.

IV) El recíproco del opuesto de todo elemento no nulo es igual al opuesto de su recíproco.

De acuerdo con 9.3.3, y por inverso multiplicativo, se tiene

$$[-(x^{-1})] \cdot (-x) = x^{-1}\, x = 1$$

Multiplicando por $(-x)^{-1}$

$$-(x^{-1})(-x)(-x)^{-1} = 1\,(-x)^{-1}$$

Por asociatividad e inversos multiplicativos resulta

$$-(x^{-1}) = (-x)^{-1}$$

V) En todo cuerpo se verifica

$$\frac{x}{y} = \frac{x'}{y'} \Leftrightarrow xy' = yx'$$

En efecto

$$\frac{x}{y} = \frac{x'}{y'} \Leftrightarrow xy^{-1} = x'\; y'^{-1} \Leftrightarrow xy^{-1}\, yy' = x'y'^{-1}yy' \Leftrightarrow$$

$$\Leftrightarrow xy' = yx'$$

## 9.10. DOMINIO DE INTEGRIDAD DE LOS ENTEROS

### 9.10.1. Relación de equivalencia en $N^2$

El lector ha tenido oportunidad de probar, en el ejercicio 3-25, la equivalencia de la relación en $N^2$ definida por

$$(a\,,\,b) \sim (a'\,,\,b') \Leftrightarrow a + b' = b + a'$$

La clase de equivalencia del elemento genérico $(a\,,\,b)$, es, por definición

$$K_{(a,b)} = \left\{(x\,,\,y) \in N^2 \,/\, (x\,,\,y) \sim (a\,,\,b)\right\}$$

Ahora bien

$$(x\,,\,y) \sim (a\,,\,b) \Rightarrow x + b = y + a$$

Se presentan tres casos

i ) $a = b \Rightarrow K_{(a,b)} = \left\{(x\,,\,y) \in N^2 \,/\, y = x\right\}$

ii ) $a < b \Rightarrow K_{(a,b)} = \left\{(x\,,\,y) \in N^2 \,/\, y = x + b - a\right\}$

iii) $a > b \Rightarrow K_{(a,b)} = \left\{(x\,,\,y) \in N^2 \,/\, y = x + a - b\right\}$

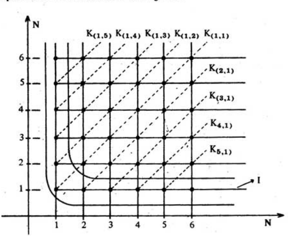
En particular

$$K_{(1,1)} = \{(1,1), (2,2), (3,3), \dots\}$$

$$K_{(1,2)} = \{(1,2), (2,3), (3,4), \dots\}$$

$$K_{(2,1)} = \{(2,1), (3,2), (4,3), \dots\}$$

La representación de las clases en $N^2$ es la siguiente




Eligiendo un único elemento en cada clase de equivalencia, se obtiene un conjunto de índices

$$I = \{(n, 1)\} \cup \{(1, n+1)\} \quad \text{con } n \in N$$

Cada clase de equivalencia se llama número entero, y el cociente $\frac{N^2}{\sim}$ es el conjunto Z de los números enteros.

***Definición***

Número entero es toda clase de equivalencia determinada por la relación definida en $N^2$.

Conjunto de los números enteros es $Z = \frac{N^2}{\sim}$

*Definición*

Número entero 0 es la clase $K_{(1,1)}$.
Entero positivo es toda clase del tipo $K_{(n,1)}$ con $n > 1$.
Entero negativo es toda clase $K_{(1,n)}$ con $n > 1$.

Para denotar los enteros utilizaremos los símbolos

$$K_{(1,1)} = 0$$
$$K_{(n,1)} = +(n-1) \qquad \text{si } n > 1$$
$$K_{(1,n)} = -(n-1) \qquad \text{si } n > 1$$

Así, $K_{(1,2)} = -1$ , $K_{(3,1)} = +2$ , etcétera.

### 9.10.2. Operaciones en $N^2$ y compatibilidad

En $N^2$ definimos la adición y multiplicación mediante

$$1.\ (a, b) + (a', b') = (a + a', b + b')$$
$$2.\ (a, b) \cdot (a', b') = (aa' + bb', ab' + ba')$$

La relación de equivalencia definida en 9.10.1. es compatible con estas leyes de composición interna en $N^2$. En efecto

i ) Por definición de la relación de equivalencia, conmutatividad y asociatividad de la adición en N, y por la definición 1., se tiene

$$(a, b) \sim (a', b') \wedge (c, d) \sim (c', d') \Rightarrow$$
$$\Rightarrow a + b' = b + a' \ \wedge \ c + d' = d + c' \Rightarrow$$
$$\Rightarrow (a + c) + (b' + d') = (b + d) + (a' + c') \Rightarrow$$
$$\Rightarrow (a + c, b + d) \sim (a' + c', b' + d') \Rightarrow$$
$$\Rightarrow (a, b) + (c, d) \sim (a', b') + (c', d')$$

ii ) Sean

$$(a, b) \sim (a', b') \wedge (c, d) \sim (c', d') \Rightarrow$$
$$\Rightarrow a + b' = b + a' \ \wedge \ c + d' = d + c'$$

Multiplicamos la primera igualdad por $c$ y luego por $d$

$$ac + b'c = bc + a'c$$
$$bd + a'd = ad + b'd$$

Sumando

$$ac + bd + a'd + b'c = bc + ad + a'c + b'd \qquad (1)$$

Multiplicando la segunda igualdád por $a'$ y por $b'$

$$a'c + a'd' = a'd + a'c'$$
$$b'd + b'c' = b'c + b'd'$$

Sumando

$$a'c + b'd + a'd' + b'c' = a'd + b'c + a'c' + b'd' \qquad (2)$$

Sumando (1) y (2), después de cancelar resulta

$$(ac + bd) + (a'd' + b'c') = (ad + bc) + (a'c' + b'd')$$

Por definición de la relación de equivalencia

$$(ac + bd\ ,\ ad + bc) \sim (a'c' + b'd'\ ,\ a'd' + b'c')$$

Por definición de producto resulta

$$(a\ ,\ b)\ .\ (c\ ,\ d) \sim (a'\ ,\ b')\ .\ (c'\ ,\ d')$$

### 9.10.3. Adición y multiplicación en Z

De acuerdo con el teorema fundamental de compatibilidad existen en el conjunto cociente $\frac{\mathbf{N}^2}{\sim} = \mathbf{Z}$ dos leyes de composición interna inducidas, llamadas suma y producto de enteros, únicas, tales que la aplicación canónica $f : \mathbf{N}^2 \to \mathbf{Z}$ es un homomorfismo.

Veamos cómo se realizan la adición y multiplicación en **Z**

$$(-3) + (+2) = f(1\ ,4) + f(3\ ,1) = f[(1\ ,4) + (3\ ,1)] = f(4\ ,5) = f(1\ ,2) = -1$$
$$(-3)\ .\ (+2) = f(1\ ,4)\ .\ f(3\ ,1) = f[(1\ ,4)\ .\ (3\ ,1)] = f(7\ ,13) = f(1\ ,7) = -6$$

Hemos utilizado la definición de aplicación canónica, el hecho de que es un homomorfismo y las definiciones de adición y multiplicación en $\mathbf{N}^2$.

Es fácil verificar que la adición es conmutativa y asociativa en $\mathbf{N}^2$, y en virtud del teorema fundamental de compatibilidad lo es en **Z**.

Además, neutro para la adición en **Z** es $0 = K_{(1,1)}$, pues

$$K_{(a,b)} + 0 = f(a\ ,b) + f(1\ ,1) = f[(a\ ,b) + (1\ ,1)] =$$
$$= f(a+1\ ,b+1) = f(a\ ,b) = K_{(a,b)}$$

El entero opuesto de $K_{(a,b)}$ es $K_{(b,a)}$ pues

$$K_{(a,b)} + K_{(b,a)} = f(a\ ,b) + f(b\ ,a) = f(a+b\ ,\ b+a) = f(1\ ,1) =$$
$$= K_{(1,1)} = 0$$

Resulta entonces que el par $(\mathbf{Z}\ ,+)$ es un grupo abeliano.

El lector puede comprobar que la multiplicación es conmutativa y asociativa en $\mathbf{N}^2$,

y por el homomorfismo canónico estas propiedades se trasfieren a la multiplicación en $\mathbf{Z}$.

Neutro para el producto en $\mathbf{Z}$ es $+1 = K_{(2,1)}$ pues

$$K_{(a,b)} \cdot K_{(2,1)} = f(a,b) \cdot f(2,1) = f[(a,b) \cdot (2,1)] =$$
$$= f(2a+b, a+2b) = f(a,b) = K_{(a,b)}$$

De manera análoga se comprueba la distributividad de la multiplicación respecto de la adición en $\mathbf{Z}$.

Por lo tanto, la terna $(\mathbf{Z}, +, .)$ es un anillo conmutativo y con unidad.

Este anillo carece de divisores de cero. En efecto

Sean los enteros $K_{(x,y)}$ y $K_{(x',y')}$ tales que

$$K_{(x,y)} \cdot K_{(x',y')} = K_{(1,1)} \quad \text{donde } K_{(x',y')} \neq 0$$

Por aplicación canónica

$$f(x,y) \cdot f(x',y') = f(1,1)$$

Por ser $f$ un homomorfismo

$$f[(x,y) \cdot (x',y')] = f(1,1)$$

Por producto en $\mathbf{N}^2$

$$f(xx'+yy', xy'+yx') = f(1,1)$$

Por definición de aplicación canónica

$$(xx'+yy', xy'+yx') \sim (1,1)$$

Teniendo en cuenta la definición de la relación de equivalencia resulta

$$xx'+yy' = xy'+yx'$$

si $x' > y'$

$$xx'-xy' = yx'-yy'$$

es decir

$$x(x'-y') = y(x'-y')$$

En consecuencia, $x = y$, y resulta $K_{(x,y)} = 0$.

Se tiene así el dominio de integridad de los números enteros.

## 9.11. ISOMORFISMO DE LOS ENTEROS POSITIVOS CON N

Sea $\mathbf{Z}^+$ el conjunto de los enteros positivos. Definimos

$$F : \mathbf{Z}^+ \to \mathbf{N}$$

mediante la asignación $F(+a) = a$.

Se verifica

i ) F es inyectiva, pues

$$+a \neq +b \Rightarrow a \neq b \Rightarrow F(+a) \neq F(+b)$$

ii ) F es sobreyectiva, ya que

$$\forall a \in \mathbf{N}, \exists +a \in \mathbf{Z}^+ / F(+a) = a$$

iii) F es un morfismo respecto de la adición en $\mathbf{Z}^+$ y en $\mathbf{N}$.

$$F[(+a)+(+b)] = F[+(a+b)] =$$
$$= a + b = F(+a) . F(+b)$$

iv) F es un morfismo respecto de la multiplicación en $\mathbf{Z}^+$ y en $\mathbf{N}$.

$$F[(+a).(+b)] = F[+(a.b)] =$$
$$= a . b = F(+a) . F(+b)$$

En consecuencia, F es un isomorfismo de $\mathbf{Z}^+$ en $\mathbf{N}$, es decir, ambos conjuntos son indistinguibles algebraicamente y pueden identificarse.

## 9.12. PROPIEDADES DEL VALOR ABSOLUTO

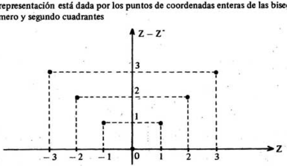
### 9.12.1. Función valor absoluto

Es la aplicación

$$f: \mathbf{Z} \to \mathbf{Z} - \mathbf{Z}^- \quad \text{definida por}$$

$$|x| = f(x) = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$$

Su representación está dada por los puntos de coordenadas enteras de las bisectrices del primero y segundo cuadrantes



### 9.12.2. Propiedades del valor absoluto

I) Todo entero está comprendido entre su valor absoluto y el opuesto de éste.

$$-|x| \leq x \leq |x|$$

Se presentan tres casos

a) $x = 0 \Rightarrow -|x| = x = |x|$

b) $x > 0 \Rightarrow -|x| < x = |x|$

c) $x < 0 \Rightarrow -|x| = x < |x|$

II) $|x| \leq a \Rightarrow -a \leq x \leq a$

En efecto

Por I)

$x \leq |x|$

Por hipótesis

$|x| \leq a$

Por transitividad resulta

$x \leq a$ (1)

Multiplicando los dos miembros de la hipótesis por $-1$

$$-|x| \geq -a$$

Por I)

$$-|x| \leq x$$

Entonces, por transitividad

$$-a \leq x \qquad (2)$$

De (1) y (2) resulta

$$-a \leq x \leq a$$

III) $-a \leq x \leq a \Rightarrow |x| \leq a$

Si $x \geq 0$, entonces por definición de valor absoluto y por hipótesis

$$|x| = x \leq a \qquad (1)$$

Si $x < 0$, por definición de valor absoluto, y multiplicando por $-1$ los dos primeros miembros de la hipótesis

$$|x| = -x \leq a \qquad (2)$$

En ambos casos, (1) y (2), se tiene

$$|x| \leq a$$

IV) El valor absoluto de una suma es menor o igual que la suma de los valores absolutos.

Tesis) $|x + y| \leq |x| + |y|$

Demostración) Por I)

$$-|x| \leqslant x \leqslant |x|$$
$$-|y| \leqslant y \leqslant |y|$$

Sumando se tiene

$$-(|x|+|y|) \leqslant x+y \leqslant |x|+|y|$$

Por III) resulta

$$|x+y| \leqslant |x|+|y|$$

V) El valor absoluto de un producto es igual al producto de los valores absolutos de los factores.

$$|x\,.\,y| = |x|\,.\,|y|$$

La demostración queda como ejercicio, y basta aplicar la definición de valor absoluto a los casos que se presentan.

## 9.13. ALGORITMO DE LA DIVISION ENTERA

**Teorema**. Dados dos enteros $a$ y $b$, siendo $b > 0$, existen dos enteros $q$ y $r$, llamados cociente y resto, que verifican

i ) $a = bq + r$

ii ) $0 \leqslant r < b$

Demostración)

Como $b$ es un entero positivo, se tiene $b \geqslant 1$ ( 1).

Multiplicando (1) por $-|a|$

$$-|a|\,b \leqslant -|a|$$

Por 9.12.2. I)

$$-|a| \leqslant a$$

De estas dos relaciones se deduce

$$-|a|\,b \leqslant a$$

En consecuencia

$$a - [-|a|\,.\,b] \geqslant 0 \qquad (2)$$

Sea C el conjunto de todos los enteros no negativos del tipo $a - xb$, con $x \in \mathbf{Z}$. De acuerdo con (2), para $x = -|a|$, se tiene

$$a - xb = a - [-|a|\,b] \geqslant 0$$

y en consecuencia C es no vacío.

Por el principio de buena ordenación existe en C un elemento mínimo $r$, para cierto valor $q$, de $x$. Es decir, existen q y $r$ tales que

$$a - bq = r \geqslant 0$$

Entonces existen dos enteros, $q$ y $r$ que satisfacen

$$a = bq + r \ \wedge \ 0 \leqslant r \qquad (3)$$

Falta probar que $r < b$. Suponemos $r \geqslant b$; en este caso

$$r - b \geqslant 0 \Rightarrow a - bq - b \geqslant 0 \Rightarrow a - b(q+1) \geqslant 0$$

$$a - b(q+1) \in C \qquad (4)$$

Y como

$$a - bq = a - bq \ \wedge \ b > 0 \Rightarrow a - b(q+1) < a - bq = r \qquad (5)$$

De (4) y (5) se infiere que C admite un elemento menor que el mínimo, lo que es absurdo. Entonces es $r < b$ (5).

Las proposiciones (3) y (5) constituyen la tesis del teorema.

Queda como ejercicio la demostración de que los enteros $q$ y $r$, a que se refiere el teorema, son únicos.

## 9.14. ALGORITMO DE EUCLIDES

### 9.14.1. Máximo común divisor en Z

El máximo común divisor positivo de dos enteros $a$ y $b$, no simultáneamente nulos, será denotado por

$$d = a \wedge b = m\,.\,c\,.\,d\,(a\,,\,b)$$

Para el máximo común divisor rige la definición 9.7.1.

Se tiene

$$3 \wedge 0 = -3 \wedge 0 = 3$$

$$-6 \wedge 3 = -6 \wedge -3 = 6 \wedge -3 = 6 \wedge 3 = 3$$

**9.14.2. Propiedad.** El máximo común divisor positivo de $a$ y $b$, siendo $b > 0$, se identifica con el máximo común divisor positivo entre $b$ y el resto de la división de $a$ por $b$.

Sean

$$A = \left\{x \in \mathbf{Z} / x \mid a \ \wedge \ x \mid b\right\}$$

y

$$B = \left\{x \in \mathbf{Z} / x \mid b \ \wedge \ x \mid r\right\}$$

Siendo

$$a = bq + r \ \wedge \ 0 \leq r < b$$

La propiedad queda satisfecha si demostramos que $A = B$.
Sea entonces

$$x \in A \Rightarrow x \mid a \ \wedge \ x \mid b \Rightarrow x \mid a \ \wedge \ x \mid b \ \wedge \ x \mid bq \Rightarrow$$
$$\Rightarrow x \mid b \ \wedge \ x \mid a - bq \Rightarrow x \mid b \ \wedge \ x \mid r \Rightarrow$$
$$\Rightarrow x \in B$$

Luego $A \subset B$ (1)
Sea ahora

$$x \in B \Rightarrow x \mid b \ \wedge \ x \mid r \Rightarrow x \mid bq \ \wedge \ x \mid r \ \wedge \ x \mid b \Rightarrow$$
$$\Rightarrow x \mid bq + r \ \wedge \ x \mid b \Rightarrow x \mid a \ \wedge \ x \mid b \Rightarrow$$
$$\Rightarrow x \in A$$

Es decir, $B \subset A$ (2)
De (1) y (2) resulta $A = B$.

### 9.14.3. Determinación del m.c.d. por el algoritmo de Euclides

Sean los enteros $a$ y $b$, con $b > 0$. Por el algoritmo de la división existen $q_1$ y $r_1$, tales que

$$a = bq_1 + r_1 \ \wedge \ 0 \leq r_1 < b$$

Por 9.14.2. se tiene $a \wedge b = b \wedge r_1$. Si $r_1 = 0$, entonces $a \wedge b = b$.

Suponemos que $r_1 > 0$, y que se llega a un resto nulo al cabo de $n + 1$ etapas, en cada una de las cuales se divide el divisor por el resto. Se tiene

$$b = r_1 q_2 + r_2 \ \wedge \ 0 < r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \ \wedge \ 0 < r_3 < r_2$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$r_{n-2} = r_{n-1} q_n + r_n \ \wedge \ 0 < r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1}$$

De acuerdo con las relaciones de la derecha podemos escribir

$$0 < r_n < r_{n-1} < r_{n-2} < \ldots < r_3 < r_2 < r_1 < b$$

donde los sucesivos restos disminuyen y son enteros no negativos. Por consiguiente se llega a un resto nulo, que aquí hemos supuesto $r_{n+1}$.

Teniendo en cuenta 9.14.2. resulta

$$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \ldots = r_{n-1} \wedge r_n = r_n \wedge 0 = r_n$$

Es decir, el máximo común divisor positivo de dos enteros no simultáneamente nulos, es igual al último resto no nulo que se obtiene por la aplicación del algoritmo de Euclides.

El esquema de las divisiones sucesivas es

| | $q_1$ | $q_2$ | $q_3$ | | $q_n$ | $q_{n+1}$ |
|---|---|---|---|---|---|---|
| $a$ | $b$ | $r_1$ | $r_2$ | .......... | $r_{n-1}$ | $r_n$ |
| $r_1$ | $r_2$ | $r_3$ | | $r_n$ | 0 | |

*Ejemplo 9-7.*

i ) El cociente y resto de la división de $-7$ por 3 son $-3$ y 2

$$\begin{array}{r|l} -7 & 3 \\ \hline 2 & -3 \end{array}$$

ii ) Si el divisor es negativo, el cociente y resto satisfacen

$$a = bq + r$$
$$0 \leqslant r < |b|$$

Así

$$\begin{array}{r|l} 7 & -3 \\ \hline 1 & -2 \end{array}$$

iii) El m.c.d. de 6060 y 66 por divisiones sucesivas se obtiene así

| | 91 | 1 | 4 | 2 |
|---|---|---|---|---|
| 6060 | 66 | 54 | 12 | 6 |
| 120<br>54 | 12 | 6 | 0 | |

Luego

$$6060 \wedge 66 = 6$$

## 9-15. NUMEROS PRIMOS

Como $( \mathbf{Z} , + , . )$ es un dominio de integridad principal trasladamos a este caso la teoría desarrollada en 9.7.

### 9.15.1. Enteros primos o irreducibles

*Definición*

El entero no nulo $p \neq \pm 1$ es primo si y sólo si los únicos divisores que admite son $+1, -1, p$ y $-p$.

***Definición***

Dos enteros son coprimos si y sólo si su máximo común divisor positivo es igual a 1.

***Ejemplo 9-8.***

i ) Si un número primo es divisor de un producto de dos factores, entonces es divisor de uno de ellos.
Está demostrado en 9.7.7.

ii ) Si un número es divisor de un producto de dos factores, y primo con uno de ellos, entonces es divisor del otro.

$$c \mid ab \ \wedge \ a \text{ y } c \text{ coprimos} \Rightarrow c \mid b$$

Demostración)

Como $a$ y $c$ son coprimos, se tiene $a \wedge c = 1$.
Por 9.7.5.

$$1 = sa + tc \Rightarrow$$

$$\Rightarrow b = sab + tcb \Rightarrow b = sqc + tbc \Rightarrow$$

$$\Rightarrow b = (sq + tb)\, c \Rightarrow c \mid b$$

iii) Si dos enteros coprimos son divisores de un tercero, entonces su producto es divisor de éste.

Hipótesis) $a \mid n$

$b \mid n$

$a \wedge b = 1$

Tesis) $a \ b \mid n$

Demostración)

$$a \mid n \Rightarrow n = a\, x \qquad (1)$$

Como

$$b \mid n \Rightarrow b \mid ax$$

y siendo $a$ y $b$ coprimos, por ii ) resulta

$$b \mid x \Rightarrow x = by \qquad (2)$$

De (1) y (2)

$$n = a\,(by) = (ab)\, y$$

O sea $a\, b \mid n$.

### 9.15.2. Factorización en Z

**Teorema.** Todo entero mayor que 1 puede descomponerse en el producto de 1 por factores primos positivos. Salvo el orden en que se consideren los factores, esta descomposición es única.

Hacemos uso del segundo principio de inducción completa, cuya demostración se pide como ejercicio. Este principio establece

Si $\forall h < m : \mathrm{P}(h) \Rightarrow \mathrm{P}(m)$, entonces $\mathrm{P}(n)$ es V, $\forall n \in \mathbf{N}$.

Consideremos ahora la proposición

$\mathrm{P}(a)$ : "El entero $a > 1$ puede descomponerse en un producto de factores primos positivos".

Suponemos que $\mathrm{P}(h)$ es V para todo $h < a$ (1)

Debemos probar que $\mathrm{P}(a)$ es V.

Si $a$ es primo, nada hay que demostrar.

Si $a$ no es primo, entonces

$$a = bc \quad \text{con} \quad b < a \ \wedge \ c < a$$

Por (1), $\mathrm{P}(b)$ y $\mathrm{P}(c)$ son proposiciones verdaderas, y por lo tanto

$b = \prod_{i=1}^{r} p'_i \wedge c = \prod_{i=1}^{s} p''_i$ siendo $p'_i$ y $p''_i$ enteros primos positivos.

Luego $a = b\,c = \prod_{i=1}^{n} p_i$, donde $n = r + s$.

Entonces: $\mathrm{P}(a)$ es V.

Tal descomposición, salvo el orden de los factores, es única. Si existieran dos descomposiciones se tendría

$$a = p_1\, p_2 \ldots p_n = q_1\, q_2 \ldots q_m$$

Como $p_1$ es primo y $p_1 | a$, por 9.7.7., se tiene $p_1 | q_j$; en consecuencia, $p_1 = q_j$, ya que son primos positivos.

Por ley cancelativa y conmutatividad

$$p_2\, p_3 \ldots p_n = q'_2\, q'_3 \ldots q'_m$$

después de ordenar el segundo miembro para que $q_j$ sea el primer factor.

Reiteramos el proceso hasta agotar los factores primos de un miembro, en cuyo caso quedan agotados los del otro. Entonces $m = n$ y la descomposición es única.

**9.15.3. Teorema de Euclides.** Existen infinitos números primos positivos.

Hipótesis) $\mathrm{S} = \{ p_i \,/\, p_i \text{ es primo} \wedge p_i > 0 \}$

Tesis) S es infinito.

Demostración)

Suponemos que S es finito. Entonces

$$S=\left\{p_1, p_2, \ldots, p_n\right\}$$

Sea

$$a=\left(\prod_{i=1}^{n} p_i\right)+1$$

Por 9.15.2. $\exists \ p_j \in S \ / \ p_j \mid a$

Si $p_j = a$, entonces existiría un número primo mayor que todo $p_i$, lo que es absurdo.

Sea

$$p_j \neq a \Rightarrow a = p_j \,.\, m \ \wedge \ m > 1$$

Luego

$$p_j \,.\, m - \left(\prod_{i=1}^{n} p_i\right) = 1$$

y como

$$\prod_{i=1}^{n} p_i = p_j \,.\, q \quad \text{, siendo } \ q = \prod_{i \neq j} p_i \,,$$

se tiene

$$p_j\, m - p_j\, q = 1$$

O sea

$$p_j\,(m-q) = 1 \Rightarrow p_j \mid 1 \Rightarrow p_j = \pm 1 \ ,$$

lo que también es absurdo.

## 9.16. EL CUERPO DE LOS RACIONALES

### 9.16.1. Relación de equivalencia en $\mathbf{Z} \times \mathbf{Z}^*$

Sea $\mathbf{Z}^* = \mathbf{Z} - \left\{0\right\}$ el conjunto de los enteros no nulos. Consideramos

$$\mathbf{Z} \times \mathbf{Z}^* = \left\{(a\,,\,b)\,/\,a \in \mathbf{Z} \ \wedge \ b \in \mathbf{Z}^*\right\}$$

Es decir, la totalidad de los pares ordenados de enteros de segunda componente no nula.

En $\mathbf{Z} \times \mathbf{Z}^*$ definimos la siguiente relación

$$(a\,,\,b) \sim (a'\,,\,b') \Leftrightarrow ab' = ba' \qquad (1)$$

Esta relación es de equivalencia, pues verifica

i ) Reflexividad.

$$(a\,,\,b) \in \mathbf{Z} \times \mathbf{Z}^* \Rightarrow ab = ba \Rightarrow (a\,,\,b) \sim (a\,,\,b)$$

ii ) Simetría.

$$(a\ ,\ b) \sim (a'\ ,\ b') \Rightarrow ab' = ba' \Rightarrow a'b = b'a \Rightarrow (a'\ ,\ b') \sim (a\ ,\ b)$$

iii) Transitividad.

$$(a\ ,\ b) \sim (a'\ ,\ b') \wedge (a'\ ,\ b') \sim (a''\ ,\ b'') \Rightarrow (a\ ,\ b) \sim (a''\ ,\ b'')$$

Se cumple trivialmente si alguna de las primeras componentes es 0.

Sea el caso en que ninguna es 0. Por (1), y ley cancelativa después de multiplicar, se tiene

$$(a\ ,\ b) \sim (a'\ ,\ b') \wedge (a'\ ,\ b') \sim (a''\ ,\ b'') \Rightarrow ab' = ba' \wedge a'b'' = b'a''$$
$$\Rightarrow a\, b'\, a'\, b'' = b\, a'\, b'\, a'' \Rightarrow a\, b'' = b\, a'' \Rightarrow (a\ ,b) \sim (a''\ ,\ b'')$$

Por el teorema fundamental de las relaciones de equivalencia existe una partición de $\mathbf{Z} \times \mathbf{Z}^*$ en clases de equivalencia, cada una de las cuales se llama número racional.

La clase de equivalencia de un elemento genérico $(a\ ,\ b)$ es

$$K_{(a,b)} = \left\{(x\ ,y) \in \mathbf{Z} \times \mathbf{Z}^*\ /\ (x\ ,y) \sim (a\ ,b)\right\}$$

Se tiene

$$(x\ ,\ y) \sim (a\ ,\ b) \Rightarrow bx = ay$$

En particular

$$K_{(1,2)} = \left\{(x\ ,y) \in \mathbf{Z} \times \mathbf{Z}^*\ /\ y = 2\,x\right\} = \left\{(x\ ,2\,x)\ /\ x \in \mathbf{Z}^*\right\}$$

donde $x$ puede tomar todos los valores enteros no nulos, y resulta

$$K_{(1,2)} = \left\{\dots\ ;\ (-2\ ,-4)\ ,(-1\ ,-2)\ ,(-1\ ,-2)\ ,(1\ ,2)\ ,(2\ ,4)\ ,(3\ ,6)\ ,\ \dots\right\}$$

Análogamente

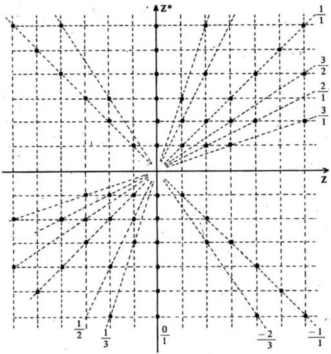
$$K_{(0,1)} = \left\{(0\ ,y)\ /\ y \in \mathbf{Z}^*\right\}$$

Es decir

$$K_{(0,1)} = \left\{\dots\ ,\ (0\ ,-2)\ ,(0\ ,-1)\ ,(0\ ,1)\ ,(0\ ,2)\ ,(0\ ,3)\ ,\ \dots\right\}$$

Es claro que, dado un elemento de $\mathbf{Z}\times\mathbf{Z}^*$, sus equivalentes se obtienen multiplicando ambas componentes por todos los enteros distintos de cero.

La representación de las clases de equivalencia es la siguiente




Un conjunto de índices está dado por la totalidad de los pares $(p, q)$ de elementos coprimos, tales que $p \in \mathbf{Z}$ y $q \in \mathbf{Z}^+$.

***Definición***

Número racional es toda clase determinada por la relación de equivalencia definida en $\mathbf{Z} \times \mathbf{Z}^*$.

Conjunto de los números racionales es el cociente de $\mathbf{Z} \times \mathbf{Z}^*$ por la relación de equivalencia

$$\mathbf{Q} = \frac{\mathbf{Z} \times \mathbf{Z}^*}{\sim}$$

Para denotar los números racionales, es decir, las clases $K_{(p,q)}$ de acuerdo con la definición del conjunto de índices, se escribe $\frac{p}{q}$ .

### 9.16.2. Operaciones en $Z \times Z^*$ y compatibilidad.

En $Z \times Z^*$ definimos la adición y multiplicación mediante

$$1.\ (a, b) + (a', b') = (ab' + ba', bb')$$
$$2.\ (a, b) \cdot (a', b') = (aa', bb')$$

Es simple la verificación de que estas leyes de composición interna en $Z \times Z^*$ son asociativas, conmutativas, y la segunda distributiva respecto de la primera.

Por otra parte, la relación de equivalencia definida en 9.16.1. es compatible con la adición y multiplicación en $Z \times Z^*$. En efecto

i ) Por la definición de la relación de equivalencia en $Z \times Z^*$

$$(a, b) \sim (c, d) \ \wedge \ (a', b') \sim (c', d') \Rightarrow ad = bc \ \wedge a'd' = b'c'$$

Multiplicando estas igualdades por $b'd'$ y $bd$, respectivamente, tenemos

$$adb'd' = bcb'd' \ \wedge \ a'd'bd = b'c'bd$$

Sumando

$$adb'd' + a'd'bd = bcb'd' + b'c'bd$$

Por distributividad en $(Z, +, .)$

$$(ab' + ba')\, dd' = (cd' + dc')\, bb'$$

Por definición de la relación de equivalencia en $Z \times Z^*$

$$(ab' + ba', bb') \sim (cd' + dc', dd')$$

Por definición 1., de adición en $Z \times Z^*$

$$(a, b) + (a', b') \sim (c, d) + (c', d')$$

Lo que prueba la compatibilidad de la relación de equivalencia respecto de la adición en $Z \times Z^*$

ii ) Aplicando la definición (1) de 9.16.1., la conmutatividad y asociatividad del producto en Z, nuevamente (1) y la definición de producto en $Z \times Z^*$, resulta

$$(a,b) \sim (a',b') \ \wedge \ (c,d) \sim (c',d')$$
$$\Downarrow$$
$$ab' = ba' \ \wedge \ cd' = dc'$$
$$\Downarrow$$
$$ab'cd' = ba'dc'$$
$$\Downarrow$$
$$(ac)(b'd') = (bd)(a'c')$$
$$\Downarrow$$
$$(ac, bd) \sim (a'c', b'd')$$
$$\Downarrow$$
$$(a,b).(c,d) \sim (a',b').(c',d')$$

Es decir, vale la compatibilidad de $\sim$ respecto del producto en $\mathbf{Z} \times \mathbf{Z}^*$.

### 9.16.3. Leyes inducidas en Q

Dado que la relación de equivalencia 9.16.1 es compatible con las leyes de composición interna definidas en $\mathbf{Z} \times \mathbf{Z}^*$, de acuerdo con el teorema fundamental de compatibilidad, existen en el conjunto cociente **Q** dos leyes de composición interna inducidas, llamadas suma y producto de racionales, únicas, tales que la aplicación canónica $f: \mathbf{Z} \times \mathbf{Z}^* \rightarrow \mathbf{Q}$ es un morfismo que preserva las propiedades.

La realización de la adición y multiplicación en **Q** es la siguiente:

$$\left(-\frac{2}{3}\right) + \frac{5}{6} = K_{(-2,3)} + K_{(5,6)} = f(-2,3) + f(5,6) =$$

$$= f[(-2,3) + (5,6)] = f(3,18) = f(1,6) = K_{(1,6)} = \frac{1}{6}$$

$$\left(-\frac{2}{3}\right) \cdot \frac{5}{6} = f(-2,3) \,.\, f(5,6) = f[(-2,3) \,.\, (5,6)] =$$

$$= f(-10,18) = f(-5,9) = -\frac{5}{9}$$

de acuerdo con la definición de aplicación canónica, el homomorfismo y las definiciones de adición y multiplicación en $\mathbf{Z} \times \mathbf{Z}^*$.

Por el mismo teorema fundamental, las operaciones inducidas en **Q** son conmutativas y asociativas. Además, la multiplicación es distributiva respecto de la adición.

Investigamos la existencia de elemento neutro para la adición en **Q**. Se trata de determinar, si existe, $K_{(x,y)}$ tal que cualquiera que sea $K_{(a,b)}$ se verifique

$$K_{(a,b)} + K_{(x,y)} = K_{(a,b)}$$

Por definición de aplicación canónica

$$f(a,b) + f(x,y) = f(a,b)$$

Por ser $f$ un homomorfismo

$$f[(a, b) + (x, y)] = f(a, b)$$

Por adición en $Z \times Z^*$

$$f(dy + bx, by) = f(a, b)$$

Por definición de aplicación canónica

$$(ay + bx, by) \sim (a, b)$$

Por 9.16.1.

$$aby + b^2x = aby$$

Cancelando en $(Z, +)$ se tiene $b^2 x = 0$, y como $b \neq 0$ resulta $x = 0$, y en consecuencia neutro para la adición en Q, es

$$K_{(0,1)} = \frac{0}{1}$$

Inverso aditivo u opuesto de $K_{(a,b)}$ es $K_{(-a,b)}$ ya que

$$K_{(a,b)} + K_{(-a,b)} = f(a, b) + f(-a, b) =$$
$$= f[(a, b) + (-a, b)] = f(ab - ab, bb) =$$
$$= f(0, bb) = f(0, 1) = K_{(0,1)} = \frac{0}{1}$$

Concluimos así que (Q , +) es un grupo abeliano.

Con relación a la multiplicación en Q, ya hemos visto que es una ley de composición interna asociativa y conmutativa. Existe elemento identidad o unidad; $K_{(1,1)} = \frac{1}{1}$ y todo racional no nulo $K_{(a,b)}$ admite inverso multiplicativo o recíproco $K_{(b,a)}$; la comprobación queda como ejercicio.

Entonces $(Q - \{0\}, .)$ es grupo abeliano.

Teniendo en cuenta, además, la distributividad de la multiplicación respecto de la adición, resulta

(Q , + , .) el cuerpo de los números racionales.

## 9.17. ISOMORFISMO DE UNA PARTE DE Q EN Z

Con $Q_1$ denotamos el conjunto de los racionales de denominador 1, es decir, todas las clases del tipo $K_{(a,1)} = \frac{a}{1}$, donde $a \in Z$.

Es fácil comprobar que la aplicación

$$f: Q_1 \to Z$$

que asigna a cada elemento de $Q_1$, el numerador, es un morfismo biyectivo respecto de la adición y multiplicación.

Esto significa que los conjuntos $Q_1$ y $Z$ son isomorfos y, en consecuencia, identificables algebraicamente.

En virtud del isomorfismo escribimos $\frac{a}{1} = a$.

## 9.18. RELACION DE ORDEN EN Q

### 9.18.1. Concepto

De acuerdo con la elección del conjunto de índices hecha en 9.16.1., todo racional puede representarse como una fracción de denominador positivo.

Definimos en Q la relación $\leqslant$ mediante

$$\frac{x}{y} \leqslant \frac{x'}{y'} \Leftrightarrow xy' \leqslant yx' \qquad (1)$$

Es claro que

$$0 \leqslant \frac{x}{y} \Leftrightarrow 0 \leqslant x \Leftrightarrow xy \geqslant 0.$$

La relación (1) satisface las propiedades reflexiva, antisimétrica y transitiva; además es total. En consecuencia (1) caracteriza un orden amplio y total en Q.

La relación $\leqslant$ es compatible con la adición y multiplicación en Q, en el sentido siguiente

i ) $\frac{a}{b} \leqslant \frac{a'}{b'} \Rightarrow \frac{a}{b} + \frac{c}{d} \leqslant \frac{a'}{b'} + \frac{c}{d}$

ii ) $\frac{a}{b} \leqslant \frac{a'}{b'} \wedge \frac{c}{d} > 0 \Rightarrow \frac{a}{b} \cdot \frac{c}{d} \leqslant \frac{a'}{b'} \cdot \frac{c}{d}$

La justificación de estas proposiciones se deja a cargo del lector. Además

$$\frac{c}{d} > 0 \Leftrightarrow 0 \leqslant \frac{c}{d} \quad \wedge \quad \frac{c}{d} \neq 0$$

Resulta entonces que la terna (Q , + , .) es un cuerpo ordenado por la relación $\leqslant$. En consecuencia, son válidas las propiedades de los anillos ordenados demostradas en 9.8.2.

### 9.18.2. Densidad de Q

***Definición***

(Relación de menor)

$$\frac{a}{b} < \frac{c}{d} \Leftrightarrow \frac{a}{b} \leqslant \frac{c}{d} \quad \wedge \quad \frac{a}{b} \neq \frac{c}{d}$$

***Definición***

Un cuerpo K es denso respecto de la relación < si y sólo si

$$x < y \Rightarrow \exists\, z \in K \,/\, x < z < y$$

**Propiedad.** El conjunto **Q** es denso con la relación <.

Se trata de probar que entre dos racionales distintos existe otro. Para esto demostramos que, sumando los numeradores y denominadores de dos racionales distintos, se obtiene otro comprendido entre los mismos.

Hipótesis)

$$\frac{a}{b} < \frac{c}{d}$$

Tesis)

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$$

Demostración)

| | |
|---|---|
| $\frac{a}{b} < \frac{c}{d}$ | Por hipótesis |
| $\Downarrow$ | |
| $ad < bc$ | Por (1) de 9.18.1 |
| $\Downarrow$ | |
| $ad + ab < bc + ab \;\wedge\; ad + cd < bc + cd$ | Por compatibilidad en (**Z** , + , . ) |
| $\Downarrow$ | |
| $a(b+d) < b(a+c) \;\wedge\; (a+c)d < (b+d)c$ | Por distributividad en (**Z** , + , .) |
| $\Downarrow$ | |
| $\frac{a}{b} < \frac{a+c}{b+d} \;\wedge\; \frac{a+c}{b+d} < \frac{c}{d}$ | Por (1) de 9.18.1 |
| $\Downarrow$ | |
| $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$ | Por transitividad |

***Ejemplo 9-9.***

Una consecuencia inmediata de la propiedad anterior, es decir, de la densidad de **Q**, es que entre dos racionales distintos se pueden intercalar infinitos si el orden está dado por la relación <.

Es claro también que no existen dos racionales consecutivos.

Podemos aplicar reiteradamente el teorema anterior en los siguientes casos:

i ) Proponer cuatro racionales entre $\frac{1}{5}$ y $\frac{2}{3}$

Resulta

$$\frac{1}{5} < \frac{3}{8} < \frac{5}{11} < \frac{7}{14} < \frac{9}{17} < \frac{2}{3}$$

Otra intercalación es

$$\frac{1}{5} < \frac{4}{13} < \frac{3}{8} < \frac{8}{19} < \frac{5}{11} < \frac{2}{3}$$

ii) Idem entre $-\frac{3}{2}$ y $\frac{3}{2}$

Se tiene

$$-\frac{3}{2} < -\frac{4}{3} < -1 < -\frac{1}{2} < 0 < \frac{3}{2}$$

## 9.19. NUMERABILIDAD DE Q

En 6.2. hemos introducido el concepto de coordinabilidad o equipotencia entre conjuntos. De acuerdo con 6.3.2. sabemos que un conjunto es numerable si y sólo si es coordinable a **N**. En el ejemplo 6-1 hemos demostrado que **Z** es numerable. Nos interesa llegar ahora a la conclusión de que **Q** también es un conjunto numerable. Con este propósito enunciamos a continuación las siguientes propiedades que se proponen como ejercicios en los Trabajos Prácticos VI y IX.

I) Todo subconjunto infinito de un conjunto numerable es numerable.

$$A \sim \mathbf{N} \ \wedge \ M \text{ es infinito} \ \wedge \ M \subset A \Rightarrow M \text{ es numerable}$$

II) La unión de un número finito de conjuntos numerables, disjuntos dos a dos, es numerable

$$A_i \sim \mathbf{N} \ \wedge \ i \in I_n \ \wedge \ A_i \cap A_j = \phi \text{ si } i \neq j \Rightarrow \sum_{i=1}^{n} A_i \text{ es numerable.}$$

III) La unión de toda familia numerable de conjuntos finitos, disjuntos dos a dos es numerable.

$$A_i \sim I_{n_i} \ \wedge \ A_i \cap A_j = \phi \text{ si } i \neq j \Rightarrow \sum_{i=1}^{\infty} A_i \text{ es numerable.}$$

IV) La unión de toda familia numerable de conjuntos numerables, disjuntos dos a dos, es numerable.

$$A_i \sim \mathbf{N} \ \wedge \ A_i \cap A_j = \phi \text{ si } i \neq j \Rightarrow \sum_{i=1}^{\infty} A_i \text{ es numerable.}$$

Con estos elementos de juicio vamos a demostrar que **Q** es numerable, en las siguientes etapas

i ) $\mathbf{Q}^+$ es numerable.

Demostración)

Sea la sucesión de conjuntos

$$A_i = \left\{ \frac{n}{i} \ / \ n \in \mathbf{N} \right\} \quad \text{con } i \in \mathbf{N}$$

Cada $A_i$ es coordinable a **N** y en consecuencia es numerable. Por ejemplo

$$A_3 = \left\{ \frac{1}{3}, \frac{2}{3}, \frac{3}{3}, \frac{4}{3}, \ldots, \frac{n}{3}, \ldots \right\}$$

De acuerdo con IV) resulta numerable el conjunto $\sum_{i=1}^{\infty} A_i$

Al prescindir de las fracciones reducibles resulta el subconjunto $\mathbf{Q}^+$, que es numerable por I), ya que consiste en un subconjunto infinito de un conjunto numerable.

ii) $\mathbf{Q}^-$ es numerable, por ser coordinable a $\mathbf{Q}^+$.

iii) **Q** es numerable.

En efecto, si denotamos con + la unión en el caso disjunto, tenemos

$$\mathbf{Q} = \mathbf{Q}^+ + \mathbf{Q}^- + \{0\}$$

Y teniendo en cuenta II y el ejemplo 2-6 resulta la numerabilidad de **Q**.

*Nota*

Los conjuntos numéricos infinitos tratados con cierto detalle hasta ahora, a saber: **N**, **Z**, enteros pares, enteros impares, enteros primos, y **Q**, son todos numerables, es decir, "tienen el mismo número de elementos". Pero no todo conjunto infinito es coordinable a **N**; en efecto, esta "tradición" no se mantiene en el caso de los números reales, conjunto que estudiaremos en el capítulo 10, donde llegaremos a la conclusión de que **R** es no numerable.

***9-10.*** **En $\mathbf{Z}^2$ se definen la adición y la multiplicación mediante**

$$(x\,,y)+(x'\,,y')=(x+x'\,,y+y')$$
$$(x\,,y)\,.\,(x'\,,y')=(xx'\,,0)$$

**Verificar que $(\mathbf{Z}^2\,,+\,,.)$ es un anillo y clasificarlo.**

***9-11.*** **Si $(A\,,+)$ es un grupo abeliano, y se define**

**$.: A^2 \to A$ tal que $a\,.\,b=0$, entonces $(A\,,+\,,.)$ es un anillo.**

***9-12.*** **En $\mathbf{Z}^2$ se consideran la suma habitual de pares ordenados y el producto definido por**

$$(a\,,b)\,.\,(a'\,,b')=(aa'\,,ab'+ba')$$

**Comprobar que $(\mathbf{Z}^2\,,+\,,.)$ es un anillo conmutativo con identidad.**

***9-13.*** **Sea $A=\left\{x\in\mathbf{R}\,/\,x=a+b\sqrt{2}\wedge a\in\mathbf{Z}\wedge b\in\mathbf{Z}\right\}$. Comprobar que A es un anillo conmutativo y con unidad con la suma y el producto ordinarios de números reales. Investigar si admite divisores de cero.**

***9-14.*** **Con relación al anillo del ejercicio anterior, verificar que**

$$f: A\to A \text{ tal que } f(a+b\sqrt{2})=a-b\sqrt{2}$$

**es un isomorfismo de A en A, respecto de la adición y de la multiplicación.**

***9-15.*** **En $A=\left\{0\,,1\,,2\,,3\right\}$ se definen la adición y multiplicación mediante las tablas**

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 0 | 3 | 2 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 2 | 1 | 0 |

| . | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 1 | 2 | 3 |

**Comprobar que $(A\,,+\,,.)$ es un anillo no conmutativo y sin identidad.**

***9-16.*** **Demostrar que la intersección de dos subanillos del anillo $(A\,,+\,,.)$ es un subanillo.**

*9-17.* Por definición, el elemento $x$ del anillo A es nilpotente si y sólo si existe $n \in \mathbf{N}$ tal que $x^n = x \,.\, x \ldots x = 0$. Demostrar que el único elemento nilpotente de todo dominio de integridad es 0.

*9-18.* Demostrar que dos enteros son congruentes módulo $n$ si y sólo si admiten el mismo resto al dividirlos por $n$.

*9-19.* Demostrar que en todo anillo ordenado se verifica

i ) $a \leqslant b \Rightarrow -b \leqslant -a$

ii ) $a \in A \Rightarrow 0 \leqslant a^2$

*9-20.* Sea el anillo ordenado $(\mathbf{Z}, +, .)$. Demostrar

i ) $|x - y| \geqslant |x| - |y|$

ii ) $\big||x| - |y|\big| \leqslant |x + y|$

iii) $x | y \;\wedge\; y \neq 0 \Rightarrow |x| \leqslant |y|$

*9-21.* Sea A un anillo. Demostrar que $I = \left\{ x \in A \,/\, nx = 0 \;\wedge\; n \in \mathbf{Z} \right\}$ es un ideal de A.

*9-22.* Demostrar que todo anillo de división carece de ideales propios no triviales.

*9-23.* En $\mathbf{R}^4$ se consideran la suma ordinaria de cuaternas ordenadas y la multiplicación definida por

$$(a_1, a_2, a_3, a_4) \,.\, (b_1, b_2, b_3, b_4) = (c_1, c_2, c_3, c_4) \quad \text{siendo}$$

$$c_1 = a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4$$
$$c_2 = a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3$$
$$c_3 = a_1 b_3 + a_3 b_1 + a_4 b_2 - a_2 b_4$$
$$c_4 = a_1 b_4 + a_4 b_1 + a_2 b_3 - a_3 b_2$$

Verificar que $\mathbf{R}^4$ es un anillo de división no conmutativo, con identidad $(1, 0, 0, 0)$. Se trata del anillo de división de los cuaterniones.
En algunos textos se considera la existencia de cuerpos no conmutativos, y en consecuencia se habla del cuerpo de los cuaterniones.

*9-24.* Resolver el siguiente sistema de ecuaciones en $(\mathbf{Z}_5, +, .)$

$$\begin{cases} \overline{2}x + \overline{1}y = \overline{2} \\ \overline{3}x + \overline{4}y = \overline{3} \end{cases}$$

*9-25.* Demostrar que si dos enteros coprimos son divisores de un tercero, entonces su producto también lo es.

*9-26.* Demostrar en $(\mathbf{Z}, +, .)$

$$m\,c\,d\,(a, b) = d \;\wedge\; a \,|\, c \;\wedge\; b \,|\, c \Rightarrow ab \,|\, cd$$

**9-27.** Expresando todo entero positivo en la forma $n = 10\, d + u$, donde $u$ denota la cifra de las unidades y $d$ el número de decenas, demostrar los siguientes criterios de divisibilidad

i ) $2 \mid u \Rightarrow 2 \mid n$

ii ) $3 \mid d + u \Rightarrow 3 \mid n$

iii) $11 \mid d - u \Rightarrow 11 \mid n$

**9-28.** Determinar el m.c.d. positivo por divisiones sucesivas, en los siguientes casos

i ) 10324 y 146 iii) 21, 3423

ii ) 1560 , − 125 iv) 215, 15, 325

**9-29.** En el anillo ordenado de los enteros se verifica

$$a \mid b \;\wedge\; |b| < a \Rightarrow b = 0$$

**9-30.** Demostrar que el cociente y el resto de la división entera son únicos.

**9-31.** Expresar el m.c.d. positivo de los enteros $a$ y $b$ como una combinación lineal adecuada de los mismos, sabiendo que se identifica con $r_2$.

**9-32.** Por definición, el entero $m$ es un mínimo común múltiplo de $a$ y $b$ si y sólo si

i ) $a \mid m \;\wedge\; b \mid m$

ii ) $a \mid m' \;\wedge\; b \mid m' \Rightarrow m \mid m'$

Si $a$ y $b$ son enteros positivos y $d$ y $m$ denotan respectivamente el m.c.d. y el m.c.m. positivos, entonces se verifica $d \,.\, m = a \,.\, b$.

**9-33.** Demostrar que si $a$ y $b$ son enteros congruentes módulo $n$, entonces $a^k$ es congruente a $b^k$ para todo $k \in \mathbf{Z}^+$.

**9-34.** Demostrar que $(\mathbf{R}^{n \times n}, +, .)$ es un anillo.

**9-35.** Demostrar el segundo principio de inducción completa citado en 9.15.2.

**9-36.** Demostrar que si $ac$ es congruente con $bc$ módulo $n$, y $c$ es coprimo con $n$, entonces $a$ es congruente con $b$ módulo $n$.

**9-37.** Sea $n$ un entero positivo. Por definición, el conjunto $\left\{a_1, a_2, \ldots, a_n\right\}$ es una clase completa de residuos módulo $n$ si y sólo si cada elemento pertenece a una clase de equivalencia determinada por la congruencia módulo $n$ en $\mathbf{Z}$.
Así, los enteros $-3$, 5 y 7 constituyen una clase completa de residuos módulo 3, pues $-3 \in \overline{0}$, $5 \in \overline{2}$ y $7 \in \overline{1}$.
Demostrar

i ) $n$ enteros constituyen una clase completa de residuos módulo $n$ si y sólo si dos elementos distintos cualesquiera no son congruentes módulo $n$.

ii ) Si $a$ y $n$ son coprimos y $\left\{a_1, a_2, \ldots, a_n\right\}$ es una clase completa de

residuos módulo $n$, entonces $\{aa_1, aa_2, \ldots, aa_n\}$ es una clase completa de residuos módulo $n$.

*9-38.* Demostrar el siguiente teorema de Fermat: si el entero primo $p$ no es divisor de $a \in \mathbf{Z}$, entonces $a^{p-1}$ es congruente con 1 módulo $p$.

*9-39.* Sean los enteros $a$, $b$ y $n$, tales que $n \in \mathbf{Z}^+$ y $a$ y $n$ son coprimos. Demostrar

i ) La ecuación de congruencia $ax \equiv b$ (mód $n$) tiene solución.

ii ) Dos enteros son soluciones de la ecuación si y sólo si son congruentes módulo $n$.

iii) Si $n$ es primo, entonces $x = a^{n-2}\, b$ es solución.

*9-40.* Resolver las siguientes ecuaciones de congruencias

i ) $3x \equiv 7 \pmod 4$

ii ) $x - 6 \equiv 0 \pmod{12}$

iii) $-2x \equiv 12 \pmod{11}$

*9-41.* Sea (K , + , .) un cuerpo. Si $b \neq 0$, entonces $ab^{-1} = \frac{a}{b}$ . Demostrar

i ) $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$

ii ) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

iii) $\frac{a}{b} = \frac{c}{d} \Rightarrow \frac{a+b}{b} = \frac{c+d}{d} \;\wedge\; \frac{a+b}{a-b} = \frac{c+d}{c-d}$

*9-42.* Demostrar que la intersección de dos subcuerpos de K es un subcuerpo.

*9-43.* Sea (Q , + , .) el cuerpo ordenado de los racionales. Demostrar

$$n \in \mathbf{N} \;\wedge\; x \in \mathbf{Q}^+ \;\wedge\; y \in \mathbf{Q}^+ \Rightarrow x^n + y^n \geqslant \frac{(x+y)^n}{2^{n-1}}$$

*9-44.* El símbolo $\mathbf{Q}(\sqrt{3})$ denota el subconjunto de números reales del tipo $a + b\sqrt{3}$, siendo $a$ y $b$ números racionales. Investigar si $(\mathbf{Q}(\sqrt{3}), +, .)$ es un cuerpo.

*9-45.* Sean (K , + , .) un cuerpo y $n$ un entero positivo. Se definen

$$0 \,.\, e = 0$$
$$1 \,.\, e = e$$
$$n \,.\, e = e + e + \ldots + e \quad \text{si } n > 1$$

donde $e$ es la unidad del cuerpo.

Demostrar

i ) $(nx)(my) = (nm)(xy)$ donde $n$ y $m$ son naturales y $x$ e $y$ son elementos de K.

ii ) $(ne)(me) = (nm)\, e$

**9-46.** Por definición, el menor entero positivo $p$ que satisface $pe = 0$ se llama característica del cuerpo. Demostrar

i ) Si $p$ es la característica de (K , + , .), entonces se verifica $px = 0$ cualquiera que sea $x \in K$.

ii ) $p$ es primo.

**9-47.** Si $p$ es la característica del cuerpo K, entonces se verifica:

$$(x+y)^p = x^p + y^p$$

**9-48.** Sea (K , + , .) un cuerpo ordenado. Por definición, K es completo si y sólo si todo subconjunto no vacío y acotado de K tiene supremo.
Por otra parte se dice que K es arquimediano si y sólo si

$$0 < x < y \Rightarrow \exists\, x \in \mathbf{N} \;/\; n x \geqslant y$$

Verificar que **Q** no es completo y sí es arquimediano.

**9-49.** Demostrar

i ) Todo subconjunto infinito de un conjunto numerable es numerable.

ii ) La unión de un número finito de conjuntos numerables, disjuntos dos a dos, es numerable.

**9-50.** Demostrar

i ) La unión de toda familia numerable de conjuntos finitos disjuntos dos a dos, es numerable.

ii ) La unión de toda familia numerable de conjuntos numerables, disjuntos dos a dos, es numerable.

Capítulo 10

# NUMEROS REALES

## 10.1. INTRODUCCION

De acuerdo con el método genérico empleado hasta ahora, se estudia en este capítulo el número real siguiendo dos vías alternativas: los encajes de intervalos cerrados racionales, y las cortaduras de Dedekind; se mencionan, además, los pares de sucesiones monótonas contiguas de racionales. Se llega a establecer que (R , + , .) es un cuerpo ordenado y completo. Asimismo, se encaran con cierto detalle la potenciación y la logaritmación en R. Se demuestra, finalmente, que R es no numerable.

## 10.2. EL NUMERO REAL

### 10.2.1. Ecuaciones sin soluciones en Q

La medida de la hipotenusa del triángulo rectángulo cuyos catetos miden 1 es $\sqrt{2}$, número que satisface la ecuación

$$x^2 - 2 = 0 \qquad (1)$$

Demostraremos que si un racional es raíz de (1), entonces dicha raíz es entera.

En efecto, sea $\frac{p}{q} \in Q$ raíz de (1), y $p$ y $q$ coprimos.

Entonces

$$\frac{p^2}{q^2} - 2 = 0 \Rightarrow p^2 - 2\,q^2 = 0 \Rightarrow p^2 = 2\,q^2 \Rightarrow q^2 \mid p^2$$

Ahora bien

$$q \mid q^2 \wedge q^2 \mid p^2 \Rightarrow q \mid p^2 \Rightarrow q \mid p \,.\, p$$

y siendo $p$ y $q$ coprimos, por 9-8 ii) resulta $q \mid p$ y en consecuencia $q = \pm 1$, es decir $\frac{p}{q} \in Z$.

Por consiguiente es válida la implicación contrarrecíproca: si la ecuación (1) no admite raíces enteras, entonces dichas raíces no son racionales.

Precisamente (1) no tiene raíces enteras, pues

$$\forall a \in Z : |a| \leqslant 1 \Rightarrow a^2 - 2 < 0$$

$$\forall a \in Z : |a| \geqslant 2 \Rightarrow a^2 - 2 > 0$$

y en consecuencia carece de raíces racionales, es decir, $\sqrt{2} \notin Q$.

Situaciones de este tipo plantean la necesidad de ampliar el conjunto Q, de modo que una parte del nuevo conjunto, que llamaremos R, sea isomorfa a Q. La vía que elegimos para este fin es el método de los intervalos encajados de racionales, a través de los cuales se tiene una representación geométrica de interés intuitivo, y, como alternativa, el de las cortaduras de Dedekind.

### 10.2.2. Encaje de intervalos cerrados racionales

***Definición***

Intervalo cerrado racional de extremos $a$ y $b$ (siendo $a \leqslant b$), es el conjunto

$$[a\,,b] = \left\{ x \in Q \;/\; a \leqslant x \leqslant b \right\}$$

De acuerdo con 9.18.2, el conjunto $[a\,,\,b] \subset Q$ es infinito, porque entre dos racionales distintos existe otro, salvo el caso $a = b$ en que el intervalo se llama degenerado y se reduce a un único elemento.

Amplitud del intervalo cerrado $[a\,,\,b]$ es el número racional $b - a$.

Sucesión de intervalos cerrados racionales es toda función $f$, con dominio N, y cuyo codominio es el conjunto de todos los intervalos cerrados racionales.

Una tal sucesión queda determinada por el conjunto de las imágenes

$$[a_1\,,a_1'\,]\,,[a_2\,,a_2'\,]\,,\,\ldots\,,[a_n\,,a_n'\,]\,,\,\ldots$$

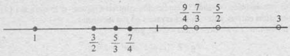
$$\text{donde } f(n) = [a_n\,,a_n']\subset Q$$

*Ejemplo 10-1.*

Los cuatro primeros términos de la sucesión cuyo elemento genérico es $\left[2 - \frac{1}{i}\,,2 + \frac{1}{i}\right]$ son los intervalos cerrados racionales

$$[1\,,3]\,,\left[\frac{3}{2}\,,\frac{5}{2}\right]\,,\left[\frac{5}{3}\,,\frac{7}{3}\right]\,,\left[\frac{7}{4}\,,\frac{9}{4}\right]$$

y su representación en un sistema de abscisas es




Esta sucesión es tal que cada intervalo está contenido en el anterior, es decir

$$[1,3] \supset \left[\frac{3}{2}, \frac{5}{2}\right] \supset \left[\frac{5}{3}, \frac{7}{3}\right] \supset \ldots$$

motivo por el cual se dice que es decreciente.

Además, la correspondiente sucesión de amplitudes $a_i' - a_i$ es convergente a 0, ya que

$$3 - 1 = 2$$

$$\frac{5}{2} - \frac{3}{2} = 1$$

$$\frac{7}{3} - \frac{5}{3} = \frac{2}{3}$$

$$\frac{9}{4} - \frac{7}{4} = \frac{1}{2}$$

Es decir, a partir de cierto índice, todos los intervalos de la sucesión tienen amplitud menor que cualquier número positivo, prefijado arbitrariamente.

La familia $\left[2 - \frac{1}{i}, 2 + \frac{1}{i}\right]$ con $i \in \mathbf{N}$ es un encaje de intervalos cerrados de racionales, concepto que precisamos a continuación.

*Definición*

Encaje de intervalos cerrados racionales es toda sucesión de intervalos cerrados racionales $[a_i, a'_i] \subset \mathbf{Q}$, con $i \in \mathbf{N}$, que satisface las siguientes condiciones:

i ) Es decreciente, en el sentido de que cada intervalo contiene al siguiente

$$i \in \mathbf{N} \Rightarrow [a_i, a_i'] \supset [a_{i+1}, a_{i+1}']$$

O bien

$$i \in \mathbf{N} \Rightarrow \mathrm{I}_{i+1} \subset \mathrm{I}_i \text{ siendo } \mathrm{I}_i = [a_i, a_i']$$

ii ) La sucesión de amplitudes es convergente a 0.

$$\forall\, \mathcal{E} > 0, \exists\, n_o(\mathcal{E}) \,/\, n > n_o \Rightarrow a_n' - a_n < \mathcal{E}$$

Es decir, prefijado cualquier número positivo $\mathcal{E}$, es posible determinar un número $n_0$ que depende de $\mathcal{E}$, tal que para todo índice de la sucesión que supere a $n_o$ ocurre que la amplitud del intervalo correspondiente es menor que $\mathcal{E}$.

***Ejemplo 10-2.***

La sucesión $\left[2-\frac{1}{i}\ ,2+\frac{1}{i}\right]$ define un encaje de intervalos, pues

i ) Es decreciente. Debemos probar $i \in \mathbf{N} \Rightarrow I_{i+1} \subset I_i$.
En efecto

$$x \in I_{i+1} \Rightarrow x \in \left[2-\frac{1}{i+1}\ ,2+\frac{1}{i+1}\right] \Rightarrow$$

$$\Rightarrow 2-\frac{1}{i+1} \leqslant x \leqslant 2+\frac{1}{1+i} \Rightarrow -\frac{1}{1+i} \leqslant x-2=\frac{1}{1+i} \Rightarrow$$

$$\Rightarrow -\frac{1}{i} < -\frac{1}{i+1} \leqslant x-2 \leqslant \frac{1}{i+1} < \frac{1}{i} \Rightarrow -\frac{1}{i} < x-2 < \frac{1}{i} \Rightarrow$$

$$\Rightarrow 2-\frac{1}{i} < x < 2+\frac{1}{i} \Rightarrow x \in \left[2-\frac{1}{i}\ ,2+\frac{1}{i}\right] \Rightarrow$$

$$\Rightarrow x \in I_i$$

ii ) La sucesión de amplitudes es convergente a 0.
Sea $\varepsilon > 0$. Hay que determinar $n_0$ tal que

$$n > n_0 \Rightarrow a_n' - a_n < \varepsilon$$

Ahora bien

$$a_n' - a_n < \varepsilon \Rightarrow \left(2+\frac{1}{n}\right) - \left(2-\frac{1}{n}\right) < \varepsilon \Rightarrow$$

$$\Rightarrow \frac{2}{n} < \varepsilon \Rightarrow n > \frac{2}{\varepsilon}$$

Afirmamos que $\forall\ \varepsilon > 0, \exists\ n_0 = \frac{2}{\varepsilon}$ tal que

$$n > n_o \Rightarrow a_n' - a_n < \varepsilon.$$

En efecto

$$n > \frac{2}{\varepsilon} \Rightarrow \frac{1}{n} < \frac{\varepsilon}{2} \Rightarrow$$

$$\Rightarrow 2+\frac{1}{n} < 2+\frac{\varepsilon}{2} \wedge 2-\frac{1}{n} > 2-\frac{\varepsilon}{2} \Rightarrow$$

$$\Rightarrow \left(2+\frac{1}{n}\right) - \left(2-\frac{1}{n}\right) < \left(2+\frac{\varepsilon}{2}\right) - \left(2-\frac{\varepsilon}{2}\right) \Rightarrow$$

$$\Rightarrow a_n' - a_n < \varepsilon$$

Analizamos algunas cuestiones de nomenclatura en conexión con los encajes de intervalos cerrados racionales.

Sea $[a_i\ ,\ a'_i]$ con $i \in \mathbf{N}$ un encaje de intervalos cerrados racionales. Entonces se verifican las condiciones

i ) $I_1 \supset I_2 \supset I_3 \supset \ldots \supset I_n \supset \ldots$

ii ) $\lim\limits_{n\to\infty} \text{ampl}\quad I_n = 0$

Los extremos inferiores $a_i$ de los intervalos del encaje se llaman aproximaciones por defecto, y los extremos superiores $a'_i$, aproximaciones por exceso.

Se verifica que las primeras constituyen una sucesión creciente de racionales. En efecto, sea $j > i$.

Por definición de encaje se tiene $I_j \subset I_i$

y como $a_j \in I_j$, resulta $a_j \in I_i$, es decir, $a_i \leqslant a_j \leqslant a'_i$ por la definición de $I_i$.

Luego

$$j > i \Rightarrow a_i \leqslant a_j$$

En consecuencia

$$a_1 \leqslant a_2 \leqslant a_3 \leqslant \ldots \leqslant a_n \leqslant \ldots$$

lo que nos dice que la sucesión de aproximaciones por defecto es creciente.

Análogamente se prueba el decrecimiento de la sucesión de las aproximaciones por exceso

$$a'_1 \geqslant a'_2 \geqslant a'_3 \geqslant \ldots \geqslant a'_n \geqslant \ldots$$

De modo que un encaje de intervalos cerrados racionales es equivalente a un par de sucesiones $\left\{a_i\right\}$ y $\left\{a'_i\right\}$ de racionales, que verifican

i ) Condición de monotonía.

$\left\{a_i\right\}$ es creciente

$\left\{a'_i\right\}$ es decreciente

ii ) $i \in \mathbf{N} \Rightarrow a_i \leqslant a'_i$

iii) Condición de contigüidad.

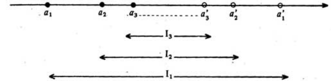
$$\forall\, \varepsilon > 0\,,\, \exists\, n_o\,(\varepsilon)\ /\ n > n_o \Rightarrow a'_n - a_n < \varepsilon$$

Se dice que $\{\, a_i \,\}$ y $\{\, a'_i \,\}$ constituyen un par de sucesiones monótonas contiguas de racionales.

Si los intervalos son no degenerados, de la condición i ) se deduce que toda aproximación por defecto del encaje es menor que cualquier aproximación por exceso. Distinguimos tres casos

1. $i = j \Rightarrow a_i < a'_i \Rightarrow a_i < a'_j$
2. $i < j \Rightarrow a_i \leqslant a_j \ \wedge\ a_j < a'_j \Rightarrow a_i < a'_j$
3. $i > j \Rightarrow a_i < a'_i \ \wedge\ a'_i \leqslant a'_j \Rightarrow a_i < a'_j$

Se tiene la siguiente representación geométrica de un encaje de intervalos cerrados racionales




La intersección de todos los intervalos del encaje puede ser vacía o no en Q. En el caso del ejemplo 10-2, se tiene

$$\bigcap_{i=1}^{\infty} \left[2 - \frac{1}{i}\ , 2 + \frac{1}{i}\right] = \{2\}$$

En cambio, el encaje asociado a las aproximaciones racionales de $\sqrt{2}$ tiene intersección vacía en Q

$$[a_1\ , a'_1] = [1\ , 2]$$
$$[a_2\ , a'_2] = [1\,.\,4\ , 1\,.\,5]$$
$$[a_3\ , a'_3] = [1\,.41\ , 1\,.\,42]$$
$$[a_4\ , a'_4] = [1\,.\,414\ , 1\,.\,415]$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\bigcap_{i=1}^{\infty} [a_i\ , a'_i] = \phi$$

### 10.2.3. Relación de equivalencia en el conjunto de los encajes de intervalos cerrados racionales. El número real.

Sea A el conjunto de todos los encajes de intervalos cerrados racionales. Cada elemento de A es una sucesión decreciente de intervalos encajados, que denotamos con $[a_i\ , a'_i]$.

En A se define la relación ~ mediante

$$[a_i\ , a'_i] \sim [b_j\ , b'_j] \Leftrightarrow a_i \leqslant b'_j \ \wedge\ b_j \leqslant a'_i \qquad \forall i\ \forall j \qquad (1)$$

Es decir, dos encajes de intervalos cerrados racionales están relacionados si y sólo si las aproximaciones por defecto de cada uno no superan a las aproximaciones por exceso del otro.

La relación definida en (1) es de equivalencia, pues satisface

I. Reflexividad.

$$[a_i\ , a'_i] \in \text{A} \Rightarrow a_i \leqslant a'_i \ \wedge\ a_i \leqslant a'_i \Rightarrow [a_i\ , a'_i] \sim [a_i\ , a'_i]$$

II. Simetría.

$$[a_i\,,\,a_i'] \sim [b_j\,,\,b_j'] \Rightarrow a_i \leqslant b_j' \;\wedge\; b_j \leqslant a_i' \Rightarrow$$
$$\Rightarrow b_j \leqslant a_i' \;\wedge\; a_i \leqslant b_j' \Rightarrow [b_j\,,\,b_j'] \sim [a_i\,,\,a_i']$$

III. Transitividad.

$$[a_i\,,\,a_i'] \sim [b_j\,,\,b_j'] \;\wedge\; [b_j\,,\,b_j'] \sim [c_k\,,\,c_k'] \Rightarrow$$
$$\Rightarrow [a_i\,,\,a_i'] \sim [c_k\,,\,c_k']$$

Demostración)
Debemos probar

$$\forall i\,,\; \forall k : a_i \leqslant c'_k \wedge c_k \leqslant a'_i$$

Suponemos que existen dos índices $m$ y $n$, tales que $a_m > c_n'$ (2)
Por hipótesis

$$[a_i\,,\,a_i'] \sim [b_j\,,\,b_j'] \Rightarrow \forall i, \forall\, j : a_i \leqslant b_j' \Rightarrow$$
$$\Rightarrow \forall j : a_m \leqslant b_j' \qquad (3)$$

$$[b_j\,,\,b_j'] \sim [c_k\,,\,c_k'] \Rightarrow \forall j\,, \forall\, k : b_j \leqslant c_k' \Rightarrow$$
$$\Rightarrow \forall j : b_j \leqslant c_n' \qquad (4)$$

Gráficamente la situación es

De (3) y (4)

$$\forall j : b_j' \geqslant a_m \;\wedge\; b_j \leqslant c_n'$$

Restando miembro a miembro

$$\forall j : b_j' - b_j \geqslant a_m - c_n'$$

y tomando $\varepsilon < a_m - c_n'$, resulta

$$\forall j : b_j' - b_j > \varepsilon$$

En consecuencia $[b_j\,,\,b'_j]$ no es un encaje, contra la hipótesis.

De acuerdo con el teorema fundamental de las relaciones de equivalencia, existe una partición de A en clases de equivalencia, cada una de las cuales se llama número real.

***Definición***

Número real es toda clase de equivalencia determinada por la relación (1) en el conjunto de todos los encajes de intervalos cerrados racionales.

Conjunto de los números reales es el cociente de A por la relación de equivalencia.

La notación $\alpha = K_{[a_i, a_i']}$ denota el número real asociado a la clase de equivalencia del encaje $[a_i, a_i']$.

Un real se llama racional si y sólo si el encaje representativo de su clase tiene intersección no vacía. Si tal intersección es vacía, el real se llama irracional.

***Definición***

Número real 0 es la clase de equivalencia de todo encaje cuyas aproximaciones por defecto no son positivas, y cuyas aproximaciones por exceso no son negativas.

El encaje $\left[-\frac{1}{i}\ ,\ \frac{1}{i}\right]$, y todos los equivalentes a él, definen el número real 0 es decir

$$0 = K_{\left[-\frac{1}{i}, \frac{1}{i}\right]}$$

***Definición***

Un número real es positivo si y sólo si todos los encajes de su clase admiten alguna aproximación por defecto positiva.

Un número real es negativo si y sólo si alguna aproximación por exceso de todos los encajes de su clase es negativa.

En símbolos

$$\alpha < 0 \Leftrightarrow \alpha = K_{[a_i, a_i']} \,/\, \exists\, a_i' < 0$$

$$\alpha > 0 \Leftrightarrow \alpha = K_{[a_i, a_i']} \,/\, \exists\, a_i > 0$$

## 10.3. OPERACIONES EN R

### 10.3.1. Operaciones en A

En el conjunto A, cuyos elementos son todos los encajes de intervalos cerrados racionales, definimos las operaciones habituales.

I. ADICION.

$$[a_i, a_i'] + [b_i, b_i'] = [a_i + b_i, a_i' + b_i']$$

La suma de dos encajes se realiza sumando las correspondientes aproximaciones por defecto y por exceso.

Esta definición satisface las condiciones que caracterizan un encaje de intervalos. En efecto

i ) Monotonía. Por ser $[a_i, a_i']$ y $[b_i, b_i']$ encajes, se verifica

$$a_i \leqslant a_{i+1} \quad \wedge \quad b_i \leqslant b_{i+1}$$

Luego

$$a_i + b_i \leqslant a_{i+1} + b_{i+1} \qquad (1)$$

Análogamente

$$a_{i+1}' + b_{i+1}' \leqslant a_i' + b_i' \qquad (2)$$

Sea ahora

$$x \in [a_{i+1} + b_{i+1}, a_{i+1}' + b_{i+1}']$$
$$\Downarrow$$
$$a_{i+1} + b_{i+1} \leqslant x \leqslant a_{i+1}' + b_{i+1}' \qquad (3)$$

De (1), (2) y (3) resulta

$$a_i + b_i \leqslant x \leqslant a_i' + b_i'$$

O sea

$$x \in [a_i + b_i, a_i' + b_i']$$

En consecuencia

$$[a_{i+1} + b_{i+1}, a_{i+1}' + b_{i+1}'] \subset [a_i + b_i, a_i' + b_i']$$

ii ) Contigüidad. Sea $\varepsilon > 0$. Por ser $[a_i, b_i]$ y $[a_i', b_i']$ encajes, existen $n_0'$ y $n_0''$ tales que

$$n' > n_0' \Rightarrow a_{n'}' - a_{n'} < \frac{\varepsilon}{2}$$

$$n'' > n_0'' \Rightarrow b_{n''}' - b_{n''} < \frac{\varepsilon}{2}$$

Para $n > n_0 = \text{máx}\left\{n_0', n_0''\right\}$ se tiene

$$a_n' - a_n < \frac{\varepsilon}{2} \quad \text{y} \quad b_n' - b_n < \frac{\varepsilon}{2}$$

Sumando

$$(a_n' + b_n') - (a_n + b_n) < 2 \cdot \frac{\varepsilon}{2} = \varepsilon$$

II. MULTIPLICACION. El producto de dos encajes queda definido por

a) $[a_i , a_i'] . [b_i , b_i'] = [a_i b_i , a_i' b_i']$ si $a_i > 0$ y $b_i > 0$ , $\forall_i$

b) $[a_i , a_i'] . [b_i , b_i'] = [a_i' b_i , a_i b_i']$ si $a_i > 0$ y $b_i' < 0$ , $\forall_i$

c) $[a_i , a_i'] . [b_i , b_i'] = [b_i , b_i']$ si $[b_i , b_i'] \sim \left[-\frac{1}{i} , \frac{1}{i}\right]$

Procediendo como en el caso I, se prueba que las definiciones II definen encajes de intervalos.

*Ejemplo 10-3.*

Determinar la suma y el producto de los siguientes pares de encajes

i ) $[a_i , a_i'] = \left[2 - \frac{1}{i} , 2 + \frac{1}{i}\right]$

$[b_i , b_i'] = \left[3 - \frac{1}{10^i} , 3 + \frac{1}{10^i}\right]$

Resulta

$$[a_i , a_i'] + [b_i , b_i'] = \left[5 - \frac{1}{i} - \frac{1}{10^i} \;,\; 5 + \frac{1}{i} + \frac{1}{10^i}\right]$$

Por otra parte, como

$$a_i b_i = 6 - \frac{3}{i} - \frac{2}{10^i} + \frac{1}{i\,10^i}$$

$$a_i' b_i' = 6 + \frac{3}{i} + \frac{2}{10^i} + \frac{1}{i\,10^i}$$

se tiene

$$[a_i , a_i'] . [b_i , b_i'] = \left[6 - \frac{3}{i} - \frac{2}{10^i} + \frac{1}{i\,10^i} \;,\; 6 + \frac{3}{i} + \frac{2}{10^i} + \frac{1}{i\,10^i}\right]$$

ii )

$$[a_i , a_i'] ,= \left[2 - \frac{1}{i} , 2 + \frac{1}{i}\right]$$

$$[b_i , b_i'] = \left[-3 - \frac{1}{i} , -3 + \frac{1}{i}\right]$$

Se tiene

$$[a_i , a_i'] + [b_i , b_i'] = \left[-1 - \frac{2}{i} , -1 + \frac{2}{i}\right]$$

Y de acuerdo con II b) el producto es

$$[a_i , a_i'] . [b_i , b_i'] = [a_i' b_i , a_i b_i'] =$$

$$= \left[ -6 - \frac{3}{i} - \frac{2}{i} - \frac{1}{i^2} \ , -6 + \frac{3}{i} + \frac{2}{i} - \frac{1}{i^2} \right] =$$

$$= \left[ -6 - \frac{5}{i} - \frac{1}{i^2} \ , -6 + \frac{5}{i} - \frac{1}{i^2} \right]$$

pues $a_i > 0 \ \wedge \ b_i' < 0$

iii) Si las aproximaciones por defecto de ambos encajes son negativas, la multiplicación se reduce al caso II a) de la siguiente manera

$$[a_i , a_i'] . [b_i , b_i'] = [-a_i' , -a_i] . [-b_i' , -b_i]$$

Así

$$\left[ -2 - \frac{1}{i} \ , -2 + \frac{1}{i} \right] . \left[ -3 - \frac{1}{i} \ , -3 + \frac{1}{i} \right] =$$

$$= \left[ 2 - \frac{1}{i} \ , 2 + \frac{1}{i} \right] . \left[ 3 - \frac{1}{i} \ , 3 + \frac{1}{i} \right] =$$

$$= \left[ 6 - \frac{5}{i} + \frac{1}{i^2} \ , 6 + \frac{5}{i} + \frac{1}{i^2} \right]$$

Si a partir de cierto índice las aproximaciones por defecto son positivas, el problema se reduce a los casos anteriores considerando

$$[a_i , a_i'] . [b_i , b_i'] = [a_j , a_j'] . [b_j , b_j']$$

siendo, para $i < j$ , $a_i < 0 \ \wedge \ a_j > 0 \ \wedge \ b_j > 0$

Si los encajes son, por ejemplo

$$[-3 , 2] , \left[ -3 + \frac{5}{2} \ , 2 \right] , \left[ -3 + \frac{5}{2} + \frac{5}{4} \ , 2 \right] , \left[ -3 + \frac{5}{2} + \frac{5}{4} + \frac{5}{8} \ , 2 \right] , \ldots$$

y $\left[ 3 - \frac{1}{i} \ , 3 + \frac{1}{i} \right]$ , es decir

$$[-3 , 2] , \left[ -\frac{1}{2} \ , 2 \right] , \left[ \frac{1}{4} , 2 \right] , \left[ \frac{7}{8} , 2 \right] , \ldots$$

$$\text{y } [2 , 4] , \left[ \frac{5}{2} , \frac{7}{2} \right] , \left[ \frac{8}{3} , \frac{10}{3} \right] , \left[ \frac{11}{4} , \frac{13}{4} \right] , \ldots$$

el producto se realiza a partir de $i = 3$ aplicando II a).

### 10.3.2. Compatibilidad

La relación de equivalencia definida en 10.2.3. es compatible con la suma y el producto definidos en 10.3.1. Lo demostramos para la adición

$$\left.\begin{array}{l}[a_i, a'_i] \sim [b_j, b'_j] \Rightarrow a_i \leqslant b'_j \ \wedge \ b_j \leqslant a'_i \\ [c_i, c'_i] \sim [d_j, d'_j] \Rightarrow c_i \leqslant d'_j \ \wedge \ d_j \leqslant c'_i\end{array}\right\} \Rightarrow$$

$$\Rightarrow a_i + c_i \leqslant b'_j + d'_j \ \wedge \ b_j + d_j \leqslant a'_i + c'_i \Rightarrow$$

$$\Rightarrow [a_i + c_i \, , \, a'_i + c'_i] \sim [b_j + d_j \, , \, b'_j + d'_j] \Rightarrow$$

$$\Rightarrow [a_i, a'_i] + [c_i, c'_i] \sim [b_j, b'_j] + [d_j, d'_j]$$

### 10.3.3. Operaciones en R

Por ser la relación de equivalencia 10.2.3. compatible con la adición y la multiplicación en A, de acuerdo con el teorema fundamental de compatibilidad, existen en el conjunto cociente **R** sendas leyes de composición interna, llamadas suma y producto de reales, únicas, tales que la aplicación canónica $f: A \to \mathbf{R}$, es un homomorfismo. Esto nos dice que para operar con dos reales se considera un encaje en cada clase de equivalencia, y se opera con éstos en A. Luego se determina la clase correspondiente al encaje obtenido.

La adición en A es asociativa y conmutativa. Estas propiedades se trasfieren a los reales con la suma.

Neutro para la adición es $0 = K\left[-\frac{1}{i}, \frac{1}{i}\right]$ pues $\forall \alpha = K_{[a_i, a'_i]}$ se verifica

$$\alpha + 0 = 0 + \alpha = K_{[a_i, a'_i]} + K_{\left[-\frac{1}{i}, \frac{1}{i}\right]} =$$

$$= f([a_i, a'_i]) + f\left(\left[-\frac{1}{i}, \frac{1}{i}\right]\right) =$$

$$= f\left([a_i, a'_i] + \left[-\frac{1}{i}, \frac{1}{i}\right]\right) = f\left(\left[a_i - \frac{1}{i}, a'_i + \frac{1}{i}\right]\right) =$$

$$= f([a_i, a'_i]) = K_{[a_i, a'_i]} = \alpha$$

$$\text{pues} \left[a_i - \frac{1}{i}, a'_i + \frac{1}{i}\right] \sim [a_i, a'_i]$$

Inverso aditivo u opuesto de $\alpha = K_{[a_i, a'_i]}$ es $-\alpha = K_{[-a'_i, -a_i]}$

En efecto

$$\alpha + (-\alpha) = (-\alpha) + \alpha = K_{[a_i, a'_i]} + K_{[-a'_i, -a_i]} =$$

$$= f([a_i, a'_i]) + f([-a'_i, a_i]) = f([a_i - a'_i, a'_i - a_i]) =$$

$$= f\left(\left[-\frac{1}{i}, \frac{1}{i}\right]\right) = 0$$

En consecuencia $(\mathbf{R}, +)$ es grupo abeliano.

Por otra parte, el producto en A es asociativo y conmutativo. **Estas propiedades** son válidas en **R**. Neutro para el producto es

$$1 = K_{[a_i, a_i']} \quad \text{tal que} \quad a_i \not> 1 \ \wedge \ a_i' \not< 1$$

Así $\quad 1 = K_{\left[1 - \frac{1}{i}, 1 + \frac{1}{i}\right]}$ y se tiene

$$\beta \,.\, 1 = 1 \,.\, \beta = K_{[b_i, b_i']} \cdot K_{\left[1 - \frac{1}{i}, 1 + \frac{1}{i}\right]} = K_{[b_i, b_i']} = \beta$$

Todo real no nulo admite inverso multiplicativo. En efecto, dado

$$\alpha = K_{[a_i, a_i']} > 0 \quad \text{con} \quad a_i > 0$$

entonces $\alpha^{-1} = K_{\left[\frac{1}{a_i'}, \frac{1}{a_i}\right]}$ es el recíproco de $\alpha$, pues

$$\alpha \,.\, \alpha^{-1} = \alpha^{-1} \,.\, \alpha = K_{\left[\frac{a_i}{a_i'}, \frac{a_i'}{a_i}\right]} = 1$$

Luego $(\mathbf{R} - \{0\}, .)$ es un grupo abeliano.

Análogamente se prueba la distributividad de la multiplicación respecto de la adición en **R**, lo que confiere a la terna $(\mathbf{R}, +, .)$ estructura de cuerpo.

***Ejemplo 10-4.***

Si

$$\alpha = K_{[a_i, a_i']} < 0$$

entonces

$$\alpha^{-1} = K_{\left[-\frac{1}{a_i}, -\frac{1}{a_i'}\right]}$$

Sea

$$[a_i, a_i'] = \left[-2 - \frac{1}{i}, -2 + \frac{1}{i}\right] = \left[\frac{-2i - 1}{i}, \frac{-2i + 1}{i}\right]$$

Se tiene

$$-\alpha = K_{[-a_i', -a_i]} = K_{\left[\frac{2i-1}{i}, \frac{2i+1}{i}\right]} > 0$$

$$\text{y} \quad (-\alpha)^{-1} = K_{\left[\frac{i}{2i+1}, \frac{i}{2i-1}\right]}$$

$$\Rightarrow \alpha^{-1} = K_{\left[\frac{-i}{2i-1}, \frac{-i}{2i+1}\right]}$$

El encaje asociado a esta clase es

$$\left[-1, -\frac{1}{3}\right], \left[\frac{-2}{3}, \frac{-2}{5}\right], \left[\frac{-3}{5}, \frac{-3}{7}\right], \ldots$$

En este caso $\quad \alpha = -2 \quad \text{y} \quad \alpha^{-1} = -\frac{1}{2}.$

## 10.4. ISOMORFISMO DE UNA PARTE DE R EN Q

Sea $R_Q$ el conjunto de los números reales definidos por clases de equivalencia asociadas a encajes de intervalos con intersección no vacía en Q. La función

$$f: R_Q \to Q$$

que asigna a cada elemento de $R_Q$ el número racional correspondiente es un morfismo biyectivo respecto de la adición y multiplicación, y en consecuencia es un isomorfismo que permite identificar algebraicamente a los conjuntos $R_Q$ y Q.

## 10.5. CUERPO ORDENADO Y COMPLETO DE LOS NUMEROS REALES

En R se define la relación $\leqslant$ mediante

$$\alpha \leqslant \beta \Leftrightarrow \exists\, \gamma \geqslant 0 \,/\, \beta = \alpha + \gamma$$

Esta definición caracteriza un orden amplio y total en R, compatible con la adición y multiplicación, es decir

i ) $\alpha \leqslant \beta \Rightarrow \alpha + \gamma \leqslant \beta + \gamma$

ii ) $\alpha \leqslant \beta \wedge \gamma \geqslant 0 \Rightarrow \alpha\gamma \leqslant \beta\gamma$

La relación $<$ se define de la siguiente manera

$$\alpha < \beta \Leftrightarrow \alpha \leqslant \beta \wedge \alpha \neq \beta$$

En R se verifica la propiedad de Arquímedes

$$0 < \alpha < \beta \Rightarrow \exists\, n \in N \,/\, \beta \leqslant n\,\alpha$$

Por otra parte, R es completo en el sentido de que todo encaje de intervalos reales define un único número real, y en consecuencia, todo subconjunto no vacío de números reales, acotado superiormente, tiene extremo superior.

Las condiciones anteriores conducen a la siguiente proposición: el cuerpo (R , + , ·) es ordenado, arquimediano y completo.

## 10.6. CORTADURAS EN Q

### 10.6.1. Concepto

Introducimos ahora un método alternativo para definir el número real a partir de Q, basado en las cortaduras de Dedekind.

*Definición*

El subconjunto $A \subset Q$ es una cortadura en Q si y sólo si verifica

i ) $A \neq \phi \wedge A \neq Q$

ii) $x \in A \wedge y < x \Rightarrow y \in A$

iii) $x \in A \Rightarrow \exists\, y | \in A \;/\; x < y$

La condición i ) significa que una cortadura en Q es una parte propia y no vacía de Q. En iii) queda especificado que A carece de máximo.

Es claro que toda cortadura en Q caracteriza una partición de Q que denotamos mediante $\left\{A, A^c\right\}$. Los elementos de $A^c$ son cotas superiores de A.

***Ejemplo 10-5.***

Los siguientes subconjuntos de Q son cortaduras

a) $A = \left\{x \in Q \;/\; x < \frac{1}{3}\right\}$

En este caso $\frac{1}{3} \in A^c$ es el extremo superior de A, es decir, el primer elemento del conjunto de las cotas superiores de A.

b) $A = Q^- \cup \left\{0\right\} \cup \left\{x \in Q^+ \;/\; x^2 < 2\right\}$

Las condiciones i ) y ii ) se satisfacen obviamente. Comprobamos que A carece de máximo utilizando la función de Dedekind

$f: Q \to Q$ definida por

$$f(x) = y = \frac{x\,(x^2+6)}{3x^2+2}$$

i) $$y - x = \frac{x\,(x^2+6)}{3x^2+2} - x = \frac{x^3 + 6x - 3x^3 - 2x}{3x^2+2} =$$

$$= \frac{4x - 2x^3}{3x^2+2} = \frac{2x\,(2-x^2)}{3x^2+2}$$

ii) $$y^2 - 2 = \frac{x^2\,(x^2+6)^2}{(3x^2+2)^2} - 2 =$$

$$= \frac{x^2\,(x^4 + 36 + 12x^2) - 2\,(9x^4 + 4 + 12x^2)}{(3x^2+2)^2} =$$

$$= \frac{x^6 - 6x^4 + 12x^2 - 8}{(3x^2+2)^2} = \frac{(x^2-2)^3}{(3x^2+2)^2}$$

iii) A no tiene máximo. En efecto, sea

$$x > 0 \;\wedge\; x \in A \Rightarrow x^2 < 2 \Rightarrow x^2 - 2 < 0$$

Siendo $x > 0$, de acuerdo con i ) y ii ) se tiene que

$$y - x > 0 \;\wedge\; y^2 - 2 < 0$$

Es decir

$$\exists\, y \in A \;/\; y > x$$

En consecuencia, A carece de máximo.
De modo análogo se prueba que B no tiene mínimo.

**10.6.2. Propiedad.** Si A es una cortadura en **Q**, entonces todo elemento de A es menor que todo elemento de $A^c$.

$$x \in A \;\wedge\; y \in A^c \Rightarrow x < y$$

En efecto, si fuera $y \leqslant x$, como $x \in A$, entonces por la condición ii ) de la **definición** resultaría $y \in A$, lo que es contradictorio con la hipótesis.

***Ejemplo 10-6.***

Todo racional $a$ determina una cortadura en **Q**, definida por

$$A = \left\{ x \in \mathbf{Q} \;/\; x < a \right\}$$

El número $a$ se llama frontera racional de la cortadura y se identifica con el mínimo de $A^c$. En el caso b) del ejemplo 10-5, no existe frontera racional.

### 10.6.3. El número real

En el conjunto de todas las cortaduras en **Q** se define la siguiente relación de equivalencia

$$A \sim B \Leftrightarrow A = B$$

Las clases de equivalencia se llaman números reales, y por ser unitarias se las identifica con la correspondiente cortadura, es decir

$$K_A = A$$

Suele utilizarse la notación $K_A = \alpha$.

En este sentido podemos decir que número real es toda cortadura en **Q**. Si la cortadura tiene frontera racional queda definido un real racional, y en caso contrario el real se llama irracional. La cortadura b) del ejemplo 10-5 define al número irracional $\sqrt{2}$.

Los conjuntos de los números reales racionales y de los reales irracionales son, respectivamente

$$\mathbf{R_Q} = \left\{ A_i \;/\; A_i \text{ es cortadura } \wedge\; A_i^c \text{ tiene mínimo} \right\}$$

$$\mathbf{R_I} = \left\{ A_i \;/\; A_i \text{ es cortadura } \wedge\; A_i^c \text{ carece de mínimo} \right\}$$

La cortadura definida por el número racional 0 es el número real 0

$$0=\left\{x \in \mathbf{Q} \ / \ x<0\right\}$$

### 10.6.4. Relación de orden en R

Sean A y B las cortaduras correspondientes a los números reales $\alpha$ y $\beta$.

***Definición***

$$\alpha<\beta \Leftrightarrow A \subset B \ \wedge \ A \neq B$$

***Definición***

El número real $\alpha$ es positivo si y sólo si $0<\alpha$

Se verifica que la definición anterior determina un orden estricto y total en **R**.

### 10.6.5. Adición en R

Sean A y B las cortaduras que definen a los números reales $\alpha$ y $\beta$. El conjunto

$$C=\left\{a+b \ / \ a \in A \ \wedge \ b \in B\right\}$$

es una cortadura en **Q**.

En efecto

i ) Por definición, es $C \neq \phi$

Además, como existen $x \in A^c \ \wedge \ y \in B^c$, por 10.6.2. se tiene

$$a<x \ \wedge \ b<y \Rightarrow a+b<x+y \Rightarrow x+y \notin C \Rightarrow x+y \in C^c$$

Luego $C^c \neq \phi$ y en consecuencia $C \neq \mathbf{Q}$

ii ) Sean

$$x \in C \ \wedge \ y<x \text{. Entonces } x=a+b \ / \ a \in A \ \wedge \ b \in B \text{.}$$

Consideremos $z \in \mathbf{Q} \ / \ y=z+b$. Como $y<x$ se tiene

$$z+b<a+b \Rightarrow z<a \Rightarrow z \in A \text{ y resulta } y \in C$$

iii) $x \in C \Rightarrow x=a+b$ tales que $a \in A \wedge b \in B$. Por ser A una cortadura, existe $z \in A$ tal que $z>a$, y en consecuencia existe $y=z+b$ en C, tal que $y>x$.

El número real $\gamma$ correspondiente a la cortadura C se llama suma de $\alpha$ y $\beta$, y puede escribirse

$$\alpha+\beta=\left\{a+b \ / \ a \in A \ \wedge \ b \in B\right\}$$

La definición propuesta caracteriza una ley de composición interna en **R**, asociativa, con neutro igual a 0, con inverso aditivo para todo elemento de **R**, y conmutativa. O sea $(\mathbf{R}, +)$ es grupo abeliano.

La cortadura correspondiente al opuesto de $\alpha$ es

$$B = -A = \left\{ x \in \mathbf{Q} \ / \ -x \text{ es cota superior no mínima de } A \right\}$$

**10.6.6. Multiplicación en R**

Dados los números reales no negativos $\alpha$ y $\beta$, definidos por las cortaduras A y B, respectivamente, consideramos el conjunto

$$C = R^- \cup \left\{ ab \ / \ a \in A \ \wedge \ b \in B \ \wedge \ a \geqslant 0 \ \wedge \ b \geqslant 0 \right\}$$

Procediendo como en 10.6.5. se prueba que C es una cortadura en **Q** y el número real que se obtiene se llama producto de $\alpha$ y $\beta$.

Esta definición se completa de la siguiente manera

$$\alpha\beta = \begin{cases} -|\alpha|\,|\beta| \text{ si } (\alpha \geqslant 0 \ \wedge \ \beta < 0) \ \vee \ (\alpha < 0 \ \wedge \ \beta \geqslant 0 \\ |\alpha|\,|\beta| \text{ si } \alpha < 0 \ \wedge \ \beta < 0 \end{cases}$$

Se demuestra que esta ley de composición interna en **R** es tal que $(\mathbf{R} - \{0\}, .)$ es grupo abeliano, y además, distributiva respecto de la adición, es decir, $(\mathbf{R}, +, .)$ es un cuerpo.

Por otra parte, la relación de orden definida en 10.6.4. es compatible con la adición y multiplicación en **R**.

Es de advertir que la operatoria con números reales sobre la base de cortaduras es inadmisible; en este sentido se recurre al método de los intervalos o de los pares de sucesiones monótonas contiguas. La ventaja de las cortaduras es esencialmente teórica.

**10.6.7. El cuerpo ordenado de los números reales**

El orden definido en 10.6.4. es compatible con la adición y multiplicación en **R**, pues verifica

i ) $\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$

ii ) $0 < \alpha < \beta \ \wedge \ 0 < \gamma \Rightarrow \alpha\gamma < \beta\gamma$

Demostramos la primera teniendo en cuenta que

$$\alpha < \beta \Rightarrow \alpha + \gamma \leqslant \beta + \gamma$$

Si fuera

$$\alpha + \gamma = \beta + \gamma$$

Por ley cancelativa en $(\mathbf{R}, +)$, resultaría $\alpha = \beta$, contra la hipótesis.

Luego

$$\alpha + \gamma < \beta + \gamma$$

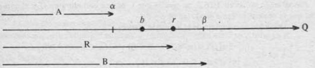
### 10.6.8. Densidad de Q en R

El conjunto **Q** es denso en **R**, pues entre dos reales distintos existe un racional, es decir

$$\alpha<\beta \Rightarrow \exists\, r \in \mathbf{Q} \ / \ \alpha<r<\beta$$

Por definición 10.6.4.

$$\alpha<\beta \Rightarrow \mathrm{A} \subset \mathrm{B} \ \wedge \ \mathrm{A} \neq \mathrm{B} \Rightarrow$$
$$\Rightarrow \exists\, b \in \mathbf{Q} \ / \ b \in \mathrm{B} \ \wedge \ b \notin \mathrm{A}$$




Sea $r>b \ \wedge \ r \in \mathrm{B}$. Considerando la cortadura R asociada a $r$, como

$$r \in \mathrm{B} \ \wedge \ r \notin \mathrm{R} \Rightarrow \mathrm{R} \subset \mathrm{B} \ \wedge \ \mathrm{R} \neq \mathrm{B} \Rightarrow$$
$$\Rightarrow r<\beta \quad (1)$$

Por otra parte

$$b \in \mathrm{R} \ \wedge \ b \notin \mathrm{A} \Rightarrow \mathrm{A} \subset \mathrm{R} \ \wedge \ \mathrm{A} \neq \mathrm{R} \Rightarrow$$
$$\Rightarrow \alpha<r \quad (2)$$

De (1) y (2) resulta

$$\exists\, r \in \mathbf{Q} \ / \ \alpha<r<\beta$$

## 10.7. COMPLETITUD DE R

### 10.7.1. Concepto

Nos proponemos demostrar que **R** es completo, lo que equivale a afirmar que todo subconjunto no vacío y acotado de **R** tiene extremo superior en **R**. Esta propiedad no es válida en **Q**, pues el subconjunto no vacío

$$\mathrm{A}=\left\{x \in \mathbf{Q}^{+} \ / \ x^{2}<2\right\} \subset \mathbf{Q}$$

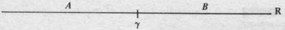
carece de extremo superior en **Q**.

**10.7.2. Teorema de Dedekind.** Si $\{A\ ,\ B\}$ es una partición de $\mathbf{R}$ que verifica

$$\alpha \in A \ \wedge\ \beta \in B \Rightarrow \alpha < \beta$$

entonces existe y es único el número real $\gamma$ que satisface

$$\alpha \leqslant \gamma \leqslant \beta \qquad \forall \alpha \in A \ \ \forall \beta \in B$$




a) Existencia.

$$\text{Sea} \quad \mathrm{C} = A \cap \mathbf{Q} = \{x \in \mathbf{Q} \ / \ x \in A\}$$

C es una cortadura en $\mathbf{Q}$. En efecto

i ) Por ser $\{A\ ,\ B\}$ una partición de $\mathbf{R}$, es

$$A \neq \phi \Rightarrow \exists\, x \in A \ / \ x \in \mathbf{Q} \Rightarrow A \cap \mathbf{Q} \neq \phi \Rightarrow$$
$$\Rightarrow \mathrm{C} \neq \phi .$$

Además, si $\beta \in B \wedge x \notin \mathrm{B}$, entonces $x \notin \mathrm{A}$ cualquiera que sea $\alpha \in A$, pues $\alpha < \beta$. Luego $x \notin \mathrm{C}$, y como $x \in \mathbf{Q}$, resulta $\mathrm{C} \neq \mathbf{Q}$.

ii ) $x \in \mathrm{C} \ \wedge\ y < x \Rightarrow \exists\, \alpha \in A \ / \ x \in \mathrm{A} \Rightarrow$

$\Rightarrow \exists\, \alpha \in A \ / \ y \in \mathrm{A} \Rightarrow y \in \mathrm{C}$

iii) $x \in \mathrm{C} \Rightarrow \exists\, \alpha \in A \ / \ x \in \mathrm{A} \Rightarrow$

$\Rightarrow \exists\, y \in A \ / \ x < y \Rightarrow y \in \mathrm{C}$

Resulta, de acuerdo con 10.6.1., que C es una cortadura en $\mathbf{Q}$, y en consecuencia queda probada la existencia del número real $\gamma$.

b) $\alpha \leqslant \gamma \leqslant \beta \qquad \forall \alpha \in A \ \ \forall \beta \in B$

Es obvio que $\alpha \leqslant \gamma$. Por otra parte, si existiera $\beta \in \mathrm{B}$ tal que $\beta < \gamma$, entonces existiría $x \in \mathbf{Q}$ tal que $x \in \mathrm{C} \wedge x \in B$.

Ahora bien

$$x \in \mathrm{C} \Rightarrow \exists\, \alpha \in A \ / \ x \in \mathrm{A}$$

y en consecuencia $\beta < \alpha$, contra la hipótesis.

c) Unicidad. Supongamos que $\gamma$ y $\gamma'$ satisfacen las condiciones del teorema, siendo $\gamma < \gamma'$. Como entre dos reales distintos existe otro $\gamma''$, se tiene

$$\left.\begin{array}{l} \gamma < \gamma'' \Rightarrow \gamma'' \in B \\ \gamma'' < \gamma' \Rightarrow \gamma'' \in A \end{array}\right\} \Rightarrow A \cap B \neq \phi$$

lo que es contradictorio con la definición de partición.

Una consecuencia inmediata del teorema es que $A$ tiene máximo, o bien $B$ tiene mínimo, pues

$$\gamma \in \mathbf{R} \Rightarrow \gamma \in A \ \vee \ \gamma \in B \Rightarrow \gamma \text{ es el máximo de } A \text{, o } \gamma \text{ es el mínimo de } B.$$

Ambas situaciones no pueden presentarse, pues $A \cap B = \phi$

**10.7.3. Teorema.** Todo subconjunto no vacío de **R** acotado superiormente tiene extremo superior.

Dado $\phi \neq X \subset \mathbf{R}$ definimos

$$A = \left\{ y \in \mathbf{R} \ / \ y < x \ \wedge \ x \in X \right\}$$

y sea $A^c = B$.

Se tiene, entonces, que ningún elemento de $A$ es cota superior de X, y, en cambio, todos los elementos de $B$ son cotas superiores de X. El teorema se reduce a probar que $B$ tiene mínimo. Observamos primero que $A$ y $B$ satisfacen las hipótesis del teorema de Dedekind

a) $z \in \mathbf{R} \Rightarrow z \in A \ \vee \ z \in B$

b) $A \cap B = \phi$

c) $X \neq \phi \Rightarrow \exists\, x \in X$

Luego

$$y < x \Rightarrow y \in A \Rightarrow A \neq \phi$$

Por otra parte, como X está acotado superiormente,

$$\exists\, y \in \mathbf{R} \ / \ x \in X \Rightarrow x \leq y \Rightarrow y \in B \Rightarrow B \neq \phi$$

Estas tres condiciones establecen que $\left\{A \ , B\right\}$ es una partición de **R**.

d) Sea ahora $\alpha \in A$. Entonces

$$\exists\, x \in X \ / \ \alpha < x$$

Si $\beta \in B$, entonces $x \leq \beta$. En consecuencia, $\alpha < \beta$, o sea

$$\alpha \in A \ \wedge \ \beta \in B \Rightarrow \alpha < \beta$$

Por el teorema mencionado existe un único número real que es el máximo de $A$, o bien el mínimo de $B$. Se trata de probar que vale esta última situación. En efecto, sea $\alpha \in A$: entonces existe $x \in X$ tal que $\alpha < x$. Ahora bien

$$\alpha < \alpha' < x \Rightarrow \alpha' \in A$$

y en consecuencia $A$ no tiene máximo.

Luego $B$ tiene mínimo y es el extremo superior de X.

## 10.8. POTENCIACION EN R

### 10.8.1. Potenciación con exponentes enteros

*Definición*

i ) $\alpha^0 = 1$ si $\alpha \in \mathbf{R} \wedge \alpha \neq 0$

ii ) $\alpha^1 = \alpha \quad \forall \alpha \in \mathbf{R}$

iii) $\alpha^{n+1} = \alpha^n \cdot \alpha$ si $n \in \mathbf{N} \wedge n \geqslant 1$

iv) $\alpha^{-n} = \left(\dfrac{1}{\alpha}\right)^n$ si $\alpha \neq 0 \wedge n \in \mathbf{N}$

### 10.8.2. Radicación de índice natural

**Teorema.** Dados $\alpha \in \mathbf{R}^+$ y $n \in \mathbf{N}$, existe un único número real positivo $\beta$ que verifica $\beta^n = \alpha$.

Demostración)

Es suficiente probar el teorema en el caso en que $\alpha < 1$. Si $\alpha > 1$, entonces existe $k \in \mathbf{Z}^+$ tal que $k > \alpha$, por la propiedad de Arquímedes. Ahora bien

$$k > \alpha \Rightarrow k^n > \alpha \Rightarrow \frac{\alpha}{k^n} < 1$$

Sea $\dfrac{\alpha}{k^n} = \alpha'$ (1). Como $\alpha' < 1$, si $\beta'$ es tal que $\beta'^n = \alpha'$, entonces para $\beta = k\,\beta'$ se tiene

$$\beta^n = k^n \beta'^n = k^n \alpha' \qquad (2)$$

Por (1)

$$\alpha = k^n \alpha' \qquad (3)$$

De (2) y (3) resulta

$$\beta^n = \alpha$$

Basta considerar pues la situación para $\alpha < 1$.

Sea

$$S = \left\{x \in \mathbf{R} \,/\, x^n \leqslant \alpha\right\}$$

Como S está acotado superiormente por 1, admite supremo. Sea éste: $\beta$.

Probaremos que $\beta^n = \alpha$. Consideremos $a \in \mathbf{R}$ tal que $|a| < 1$, y sea

$$(\beta + a)^n = \sum_{i=0}^{n} \binom{n}{i} \beta^{n-i} a^i =$$

$$= \beta^n + \sum_{i=1}^{n} \binom{n}{i} \beta^{n-i} a^i =$$

$$= \beta^n + a \sum_{i=1}^{n} \binom{n}{i} \beta^{n-i} a^{i-1}$$

Entonces

$$(\beta + a)^n - \beta^n = a \sum_{i=1}^{n} \binom{n}{i} \beta^{n-i} a^{i-1}$$

Tomando módulos

$$|(\beta + a)^n - \beta^n| = |a| \,.\, |\sum_{i=1}^{n} \binom{n}{i} \beta^{n-i} a^{i-1}|$$

Por módulo de la suma y del producto se tiene

$$|(\beta + a)^n - \beta^n| \leqslant |a| \sum_{i=1}^{n} \binom{n}{i} \beta^{n-i} |a|^{i-1}$$

Y como $|a| < 1$, resulta

$$|(\beta + a)^n - \beta^n| < |a| \sum_{i=1}^{n} \binom{n}{i} \beta^{n-i}$$

Haciendo $\sum_{i=1}^{n} \binom{n}{i} \beta^{n-i} = b$ nos queda

$$|(\beta + a)^n - \beta^n| < b\,|a|$$

Si fuera $\beta^n < \alpha$, definiendo

$$a = \frac{\alpha - \beta^n}{b}$$

como $\alpha < 1$ y $b > 1$, resulta $0 < a < 1$.

Entonces

$$0 < (\beta + a)^n - \beta^n < b \cdot \frac{\alpha - \beta^n}{b} = \alpha - \beta^n \Rightarrow$$

$$\Rightarrow (\beta + a)^n - \beta^n < \alpha - \beta^n \Rightarrow$$

$$\Rightarrow (\beta + a)^n < \alpha \Rightarrow \beta + a \in S$$

Es decir, a S pertenece el número real $\beta + a$, que es mayor que el supremo $\beta$, lo que es absurdo.

De modo que no es posible que

$$\beta^n < \alpha$$

Análogamente se deduce la imposibilidad de que

$$\beta^n > \alpha$$

Resulta entonces

$$\beta^n = \alpha$$

Ahora bien, $\beta$ es único, pues si existiera $\beta' \neq \beta$ en $\mathbf{R}^+$, tal que $\beta'^n = \alpha$, se presentarían dos alternativas

i) $0 < \beta' < \beta \Rightarrow \alpha = \beta'^n < \beta^n = \alpha \Rightarrow$

$\Rightarrow \alpha < \alpha$

ii) $0 < \beta < \beta' \Rightarrow \alpha = \beta^n < \beta'^n = \alpha \Rightarrow$

$\Rightarrow \alpha < \alpha$

lo que es absurdo. Luego, $\beta$ es el único número real positivo que verifica

$$\beta^n = \alpha$$

*Definición*

$\beta$ es la raíz $n$-sima aritmética exacta de $\alpha \in \mathbf{R}^+$

La notación es

$$\beta = \sqrt[n]{\alpha} = \alpha^{\frac{1}{n}}$$

Se presentan los siguientes casos:

a) Si $\alpha > 0$ y $n$ es par, entonces existen dos raíces $n$-simas en $\mathbf{R}$.

$$\beta_1 = \sqrt[n]{\alpha} \wedge \beta_2 = -\sqrt[n]{\alpha}$$

b) Si $\alpha < 0$ y $n$ es par, no existe $\sqrt[n]{\alpha}$

c) Si $\alpha < 0$ y $n$ es impar, entonces

$$\beta = -\sqrt[n]{-\alpha} \quad \text{es tal que} \quad \beta < 0 \wedge \beta^n = \alpha$$

### 10.8.3. Propiedades de la radicación con índice natural

Sean

$$\alpha \in \mathbf{R}^+ \wedge \beta \in \mathbf{R}^+$$

I. $\sqrt[n]{\alpha \beta} = \sqrt[n]{\alpha}\,\sqrt[n]{\beta}$

En efecto

$$\sqrt[n]{\alpha} = x \wedge \sqrt[n]{\beta} = y \quad \text{por 10.8.2.}$$

$$\Downarrow$$

$$\alpha = x^n \wedge \beta = y^n$$

$$\Downarrow$$

$$\alpha \beta = (x y)^n$$

$$\Downarrow$$

$$\sqrt[n]{\alpha \beta} = x y$$

$$\Downarrow$$

$$\sqrt[n]{\alpha \beta} = \sqrt[n]{\alpha}\,\sqrt[n]{\beta}$$

II. $\alpha : \beta = \gamma \Rightarrow \sqrt[n]{\alpha : \beta} = \sqrt[n]{\alpha} : \sqrt[n]{\beta}$

$$\alpha : \beta = \gamma$$

$$\gamma \cdot \beta = \alpha$$

$$\sqrt[n]{\gamma}\sqrt[n]{\beta} = \sqrt[n]{\alpha}$$

$$\sqrt[n]{\gamma} = \sqrt[n]{\alpha} : \sqrt[n]{\beta}$$

$$\sqrt[n]{\alpha : \beta} = \sqrt[n]{\alpha} : \sqrt[n]{\beta}$$

III. $\sqrt[m]{\sqrt[n]{\alpha}} = \sqrt[mn]{\alpha}$

IV. $\sqrt[n]{\alpha^m} = \sqrt[np]{\alpha^{mp}}$ si $p \in \mathbf{N}$

Las demostraciones de estas dos propiedades se proponen como ejercicios.

### 10.8.4. Potenciación con exponente racional

***Definición***

$$\alpha^{\frac{m}{n}} = \sqrt[n]{\alpha^m} \quad \text{si} \quad \frac{m}{n} \in \mathbf{Q}^+ \;\; \text{y} \;\; \alpha \in \mathbf{R}^+.$$

Si $\alpha < 0$, entonces existe $\alpha^{\frac{m}{n}}$ para $n$ impar.

***Definición***

$$\alpha^{-\frac{m}{n}} = \left(\frac{1}{\alpha}\right)^{\frac{m}{n}} = \frac{1}{\sqrt[n]{\alpha^m}} \quad \text{si} \quad \alpha \neq 0$$

y $\frac{m}{n} \in \mathbf{Q}^+$.

Para $\alpha < 0$ vale la restricción: $n$ impar.

***Ejemplo 10-7.***

Demostrar la regla del producto de potencias de igual base.

$$\alpha^{\frac{m}{n}} \cdot \alpha^{\frac{p}{q}} = \sqrt[n]{\alpha^m} \cdot \sqrt[q]{\alpha^p} =$$
$$= \sqrt[nq]{\alpha^{mq}}\ \sqrt[nq]{\alpha^{pn}} = \sqrt[nq]{\alpha^{mq+pn}} =$$
$$= \alpha^{\frac{mq+pn}{nq}} = \alpha^{\frac{m}{n}+\frac{p}{q}}$$

### 10.8.5. Potenciación con exponente real

Sean $\alpha > 0$ y $\beta \in \mathbf{R}$.

i ) $\alpha > 1$

$\beta$ está definido por el encaje de intervalos cerrados racionales $[b_i , b_i']$

Se tiene

$$b_1 \leqslant b_2 \leqslant b_3 \leqslant \ldots \leqslant b_3' \leqslant b_2' \leqslant b_1'$$

Como $\alpha > 1$, resulta

$$\alpha^{b_1} \leqslant \alpha^{b_2} \leqslant \alpha^{b_3} \leqslant \ldots \leqslant \alpha^{b_3'} \leqslant \alpha^{b_2'} \leqslant \alpha^{b_1'}$$

Además, $\forall\, \mathcal{E} > 0,\ \exists\, n_0$ tal que

$$n > n_0 \Rightarrow \alpha^{b_n'} - \alpha^{b_n} = \alpha^{b_n} (\alpha^{b_n' - b_n} - 1) < \mathcal{E}$$

En consecuencia

$$[\alpha^{b_i} , \alpha^{b_i'}]$$

es un encaje de intervalos cerrados en $\mathbf{R}$ que define al único número real $\alpha^{\beta}$.

ii ) Para $\alpha < 1$, el encaje

$$[\alpha^{b_i'} , \alpha^{b_i}] = \alpha^{\beta}$$

## 10.9. LOGARITMACION EN R⁺

### 10.9.1. Concepto

Dados $a \in \mathbf{R}^+$, $b \in \mathbf{R}^+$ y $b \neq 1$, existe un único número real $x$ tal que verifica

$$b^x = a$$

$x$ se llama logaritmo de $a$ en base $b$.

*Definición*

$$\log_b a = x \Leftrightarrow b^x = a$$

### 10.9.2. Propiedades. Sean $m \in \mathbf{R}^+$, $n \in \mathbf{R}^+$, $b \in \mathbf{R}^+$ y $b \neq 1$.

I. Logaritmo del producto.

Sean

$$\log_b m = x \;\wedge\; \log_b n = y$$
$$\Downarrow$$
$$b^x = m \;\wedge\; b^y = n$$
$$\Downarrow$$
$$b^{x+y} = m\,n$$
$$\Downarrow$$
$$\log_b (m\,n) = x + y$$
$$\Downarrow$$
$$\log_b (m\,n) = \log_b m + \log_b n$$

II. Logaritmo del cociente.

$$\log_b (m : n) = \log_b m - \log_b n$$

III. Logaritmo de una potencia.

$$\log_b m^\alpha = \alpha \log_b m$$

IV. Invarianza

$$\log_b m = x \;\wedge\; \alpha \neq 0 \Rightarrow \log_{b^\alpha} m^\alpha = x$$

### 10.9.3. Cambio de base

Si $b = 10$, los logaritmos se llaman decimales y la notación es

$$\log_{10} m = \log m$$

Si la base es $b = e = 2{,}718281\ldots$, los logaritmos se llaman naturales y se denotan por

$$\log_e m = \ln m = \lg m$$

Dado el $\ln a$, nos interesa obtener $\log_b a$.
Sea

$$\log_b a = x \Rightarrow b^x \Rightarrow a \Rightarrow$$
$$\Rightarrow x \ln b = \ln a \Rightarrow x = \frac{1}{\ln b} \,.\ln a \Rightarrow$$
$$\Rightarrow \log_b a = \frac{1}{\ln b} \,.\ln a$$

En el caso $b = 10$, se tiene

$$\frac{1}{\ln 10} = 0{,}434294\ldots$$

y resulta

$$\log a = 0{,}434294\ldots \ln a$$

## 10.10. POTENCIA DEL CONJUNTO R

Nos proponemos demostrar lo que hemos anticipado en 9.19: el conjunto de los números reales es no numerable. El número cardinal correspondiente a **R** se llama potencia del continuo y se denota por $c$.

**10.10.1. Teorema.** El intervalo cerrado $[0 , 1]$ es no numerable.

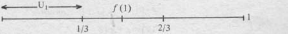
Suponemos que $[0 , 1]$ es numerable. Esto significa que $\mathbf{N} \sim [0 , 1]$, y en consecuencia, por definición de coordinabilidad, existe

$$f : \mathbf{N} \rightarrow [0 , 1] \text{ tal que } f \text{ es biyectiva.}$$

Por ser $f$ sobreyectiva, la imagen de **N** se identifica con $[0 , 1]$, es decir

$$[0 , 1] = \{f(1), f(2), f(3), \ldots\}.$$

Sea $[0 , 1] = \mathrm{U}$. Mediante los puntos de abscisas $1/3$ y $2/3$ subdividimos a U en tres subintervalos de igual amplitud




Ahora bien: $f(1)$ pertenece a lo sumo a dos de los tres subintervalos. En este caso, seleccionamos aquel subintervalo al cual no pertenece $f(1)$. Pero si pertenece a uno solo, elegimos, entre los dos a los que no pertenece, al de la izquierda. Queda así caracterizado $\mathrm{U}_1$ tal que

$$f(1) \notin \mathrm{U}_1$$

Subdividimos a éste en tres partes iguales, y con el mismo procedimiento seleccionamos $\mathrm{U}_2$ tal que

$$f(2) \notin \mathrm{U}_2$$

Análogamente, para $f(3)$ queda definido $\mathrm{U}_3$ de modo que

$$f(3) \notin \mathrm{U}_3$$

Se tiene así una sucesión de intervalos $\mathrm{U}_1, \mathrm{U}_2, \mathrm{U}_3, \ldots$ que verifica

i ) $\mathrm{U}_1 \supset \mathrm{U}_2 \supset \mathrm{U}_3 \supset \ldots$ tales que $\forall n : f(n) \notin \mathrm{U}_n$

ii) Como la amplitud de $U_n$ es $\frac{1}{3^n}$, se tiene que la sucesión de las amplitudes es convergente a 0.

En consecuencia, se trata de un encaje de intervalos cerrados en **R**, que como sabemos define a un único número real $x_0 \in U$, siendo

$$\{x_o\} = \bigcap_{i \in \mathbf{N}} U_i$$

Como $f$ es biyectiva, dado $x_0 \in U$, existe $n_0 \in \mathbf{N}$ tal que

$$f(n_o) = x_o \in U_n \qquad \text{para todo } n \in \mathbf{N}$$

Pero por la elección de los $U_n$, $f(n_0) = x_0 \notin U_{n_0}$, proposición que es contradictoria con la anterior. Luego, $[0\,,\,1]$ es no numerable.

### 10.10.2. Teorema.

Si $a < b$, entonces $[a\,,\,b]$ es coordinable a $[0\,,\,1]$.

Basta definir

$$f : [0\,,1] \to [a\,,b] \qquad \text{mediante}$$

$$f(x) = a + x\,(b - a)$$

Es inmediato que $f$ resulta biyectiva, y en consecuencia $[a\,,\,b] \sim [0\,,1]$.

### 10.10.3. Potencia de R

Por definición, el conjunto A tiene potencia $c$ si y sólo si A es coordinable a $[0\,,\,1]$. Se proponen como ejercicios, las demostraciones de las siguientes propiedades:

i ) Si $a < b$, entonces $(a\,,\,b) \sim [0\,,\,1]$

ii) La unión disjunta de un número finito de conjuntos de potencia $c$ tiene potencia $c$.

$$c(A_i) = c \Rightarrow \sum_{i=1}^{n} A_i \sim [0\,,\,1]$$

iii) Toda unión numerable de conjuntos disjuntos de potencia $c$ tiene potencia $c$.

$$c(A_i) = c \Rightarrow \sum_{i \in \mathbf{N}} A_i \sim [0\,,\,1]$$

En el ejemplo 4-20 hemos demostrado que la función $f : \mathbf{R} \to (-1\,,\,1)$ definida por

$$f(x) = \frac{x}{1 + |x|}$$

es biyectiva.

**Luego**

$$\mathbf{R} \sim (-1 \, , 1)$$

**Por** i )

$$(-1 \, , 1) \sim [0 \, , 1]$$

Por transitividad resulta $\mathbf{R} \sim [0 \, , 1]$ y en consecuencia

$$c\ (\mathbf{R}) = c\ ([0 \ , \ 1]) = c$$

## TRABAJO PRACTICO X

***10-8.*** Demostrar que si la ecuación con coeficientes enteros

$$x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

tiene raíces racionales, entonces dichas raíces son enteras.

***10-9.*** Utilizando el contrarrecíproco del teorema anterior, demostrar

i ) $\sqrt{5}$ no es racional

ii ) La razón entre la diagonal de un cubo y su arista no es racional.

***10-10.*** Demostrar que toda raíz entera de la ecuación del ejercicio 10-8 divide al término independiente.

***10-11.*** Demostrar que la ecuación $3x^3 - x = 1$ carece de raíces en **Q**.

***10-12.*** Demostrar que $\sqrt{2} + \sqrt{5}$ es irracional.

***10-13.*** Verificar que $\left[3\ ,\ 3 + \frac{1}{i}\right]$ y $\left[3 - \frac{1}{10^i}\ ,\ 3 + \frac{1}{10^i}\right]$ son encajes de intervalos cerrados racionales equivalentes.

***10-14.*** Determinar las tres primeras aproximaciones por defecto y por exceso de los encajes que definen a $\sqrt{2}$ y $\sqrt{5}$, y efectuar

$$\sqrt{2}+\sqrt{5}\ ,\ \sqrt{2}-\sqrt{5}\ ,\ \sqrt{2}\,.\,\sqrt{5}\ \text{ y }\ \sqrt{2}:\sqrt{5}$$

***10-15.*** Obtener las cortaduras en **Q** que definen a $\sqrt{3}$ y a $\sqrt{5}$.

***10-16.*** Obtener los subconjuntos de **R** que satisfacen a

i ) $|x+2| \leq 2$ iii) $x^2 < 5$ v ) $x^3 < x$

ii ) $|x+2| > 1$ iv) $x^2 \geq 5$ vi) $(x+2)(x-1)(x-2)x < 0$

Determinar en cada caso la existencia de cotas y de extremos.

***10-17.*** Comparar los números $\sqrt{2} + \sqrt{3}$ y $\sqrt{5}$, y si son distintos determinar el menor.

***10-18.*** Sea $X = \left\{x = \frac{1}{n} \,/\, n \in \mathbf{N}\right\}$. Verificar que X está acotado y determinar, si existen, el supremo y el ínfimo en **Q**.

*10-19.* Estudiar la acotación y la existencia de extremos de los conjuntos

i ) $A = \{ x \in \mathbf{R}^+ \ / \ x^2 < 2 \}$

ii ) $B = \{ x \in \mathbf{R} \ / \ x^2 > 2 \}$

iii) $C = \{ x \in \mathbf{R}^+ \ / \ x^2 > 2 \}$

*10-20.* Sean A y B dos subconjuntos acotados de **R** tales que $a = \sup A$ y $b = \sup B$. Demostrar que el supremo de

$$C = \{ x + y \ / \ x \in A \ \wedge \ y \in B \}$$

es $a + b$.

*10-21.* Determinar los extremos de

$$A = \{ x \in \mathbf{R} \ / \ 3x^2 - 2x - 1 < 0 \}$$

*10-22.* Sea $A \subset \mathbf{R}$ y acotado. Demostrar

$$a = \operatorname{Sup} S \ \wedge \ \varepsilon > 0 \ \Rightarrow \ \exists \, x \in A \ / \ a - \varepsilon < x \leqslant a$$

*10-23.* Demostrar las propiedades III y IV que figuran en 10.8.3.

*10-24.* Demostrar las propiedades i ), ii ) y iii) enunciadas en 10.10.3.

*10-25.* i ) Efectuar

$$\sqrt{\left(\sqrt{2}+\sqrt{3}+\sqrt{5}\right)\left(\sqrt{2}-\sqrt{3}-\sqrt{5}\right)\left(\sqrt{3}-\sqrt{2}-\sqrt{5}\right)\left(\sqrt{2}+\sqrt{3}-\sqrt{5}\right)}$$

ii ) Comparar

$$\log_2 5 \ \text{ y } \ \log_{1/2} \frac{1}{5}$$

*10-26.* i ) Calcular

$$\sqrt{\sqrt{2}} + 2\sqrt[8]{4} - \sqrt[4]{32}$$

ii ) Determinar los recíprocos de

$$\sqrt{3} - \sqrt{2} \ ; \ 1 + \sqrt{5} - \sqrt{2}$$

*10-27.* Resolver las ecuaciones en **R**

i ) $$\log_{\sqrt{2}} x + \log_{2\sqrt{2}} (2x) - 2 \log_2 x = 1$$

ii ) $$3^x \, 4^x - 1 = \left(\frac{1}{11}\right)^{-1}$$

*10-28.* Resolver en **R**

$$4^{y+1} - 3 \cdot 4^y - 1 = 0$$

*10-29.* Determinar $x \in \mathbf{R}^+$ sabiendo que

$$x^{\sqrt{x}} - (\sqrt{x})^x = 0$$

***10-30.*** Resolver el sistema

$$\begin{cases} \log_x y + \log_y x = \dfrac{4}{3} \\ x \, . \, y = 16 \end{cases}$$

Capítulo 11

# EL CUERPO DE LOS NUMEROS COMPLEJOS

## 11.1 INTRODUCCION

Presentamos en esta unidad la teoría y la ejercitación básicas relativas al estudio de los números complejos. La generación del conjunto C y de las operaciones en él es la habitual: una relación de equivalencia en $R^2$ que presenta la ventaja de caracterizar clases unitarias y la consiguiente identificación con C. Se definen las operaciones de adición y de multiplicación, se destaca el isomorfismo de una parte de C en R, y además de la forma binómica se introducen las formas trigonométrica y exponencial. Queda resuelto el problema de la radicación y de la logaritmación, no siempre posibles en R. Se introduce, además, el concepto de raíces primitivas de la unidad.

## 11.2. EL NUMERO COMPLEJO

### 11.2.1. Ecuaciones sin soluciones en R

El ejemplo más conspicuo de una ecuación sin raíces reales es

$$x^2 + 1 = 0$$

ya que, cualquiera que sea $x \in R$, se verifica $x^2 \geqslant 0$, y en consecuencia

$$x^2 + 1 > 0$$

De un modo más general, la ecuación $ax^2 + bx + c = 0$ con coeficientes reales no tiene soluciones en R si el discriminante $b^2 - 4ac$ es negativo.

Se hace necesaria la ampliación de R a un conjunto en el cual puedan resolverse situaciones del tipo anterior, de manera que R sea isomorfo a una parte de él. Tal conjunto es el de los números complejos.

### 11.2.2. Relación de equivalencia en $R^2$ y números complejos

En el conjunto $R^2$, de todos los pares ordenados de números reales, definimos la relación $\sim$ mediante

$$(a, b) \sim (c, d) \Leftrightarrow a = c \wedge b = d$$

Esta relación es la identidad, y obviamente es de equivalencia; se traduce en el siguiente enunciado: "dos pares ordenados de números reales son equivalentes si y sólo si son idénticos".

Cada clase de equivalencia es unitaria, y se la identifica con el par ordenado correspondiente, es decir

$$K_{(a,b)} = \{(a, b)\}$$

La identificación que proponemos, en virtud del unitarismo de las clases nos permite escribir

$$K_{(a,b)} = (a, b)$$

***Definición***

Número complejo es todo par ordenado de números reales.

El conjunto de los números complejos es $C = R^2$.

Es decir

$$C = \{(a, b) \ / \ a \in R \wedge b \in R\}$$

La notación usual para los números complejos es $z = (a, b)$.

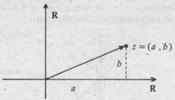
***Definición***

Parte real de un número complejo es su primera componente. Parte imaginaria, su segunda componente.

Conviene advertir que las partes real e imaginaria de un complejo son números reales. Las notaciones son

$$Re(z) = a \wedge Im(z) = b$$

Introduciendo un sistema cartesiano, los números complejos se corresponden con los puntos del plano. La abscisa de cada punto es la parte real, y la ordenada es la parte imaginaria. Por otro lado, a cada complejo le está asociado un vector con origen en el origen del sistema, y cuyo extremo es el punto determinado por el par ordenado correspondiente.




Los complejos de parte imaginaria nula, es decir, los pares ordenados del tipo $(a, 0)$, son puntos del eje de abscisas. Los complejos de parte real nula caracterizan el eje de ordenadas.

***Definición***

Un complejo es real si y sólo si su parte imaginaria es cero.
Un complejo es imaginario si y sólo si su parte real es cero.

***Ejemplo 11-1.***

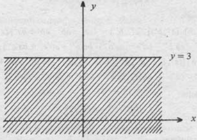
Determinamos analítica y gráficamente los complejos $z = (x, y)$ que verifican

i ) $Re(z) = 2$

Resultan todos los pares ordenados para los cuales $x = 2$, es decir, $z = (2, y)$. La ecuación $x = 2$ corresponde a la recta paralela al eje de ordenadas que pasa por el punto de abscisa 2.

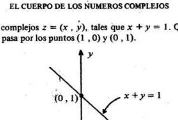
ii ) $Im(z) \leqslant 3$

La condición anterior se traduce en $y \leqslant 3$, y corresponde al semiplano que contiene al origen, cuyo borde es la recta de ecuación $y = 3$.




iii) $Re(z) + Im(z) = 1$

Se trata de los complejos $z = (x\,,y)$, tales que $x + y = 1$. Queda definida así la recta del plano que pasa por los puntos $(1\,,0)$ y $(0\,,1)$.




### 11.2.3. Operaciones en C

En $\mathbf{C} = \mathbf{R}^2$ se definen la adición y multiplicación mediante

1. $(a\,,b) + (c\,,d) = (a + c\;,\;b + d)$
2. $(a\,.\,b)\;.\;(c\,,d) = (a\,c - b\,d\,,\;a\,d + b\,c)$

Estas leyes de composición interna en C verifican las siguientes propiedades:

I) $(\mathbf{C}\,,+)$ es un grupo abeliano. La justificación está dada en los ejemplos 5-2 y 5-5. Complejo nulo es el par $(0\,,0)$, y el inverso aditivo de todo complejo $z = (a\,,b)$ es $-z = (-a\,,-b)$

II) $(\mathbf{C} - \{0\}\,,.)$ es un grupo abeliano. El símbolo 0 denota el complejo nulo $(0\,,0)$. Verificamos los axiomas

$G_1$ : El producto es ley de composición interna en **C**, por la definición 2.

$$z \in \mathbf{C} \;\wedge\; z' \in \mathbf{C} \Rightarrow z\,.\,z' \in \mathbf{C}$$

$G_2$ : Asociatividad.

$$(z\,.\,z')\,.\,z'' = [(a\,,b)\,.\,(a'\,,b')]\,.\,(a''\,,b'') = (aa' - bb'\,,\;ab' + ba')\,(a''\,,b'') =$$
$$= (aa'a'' - bb'a'' - ab'b'' - ba'b''\,,aa'b'' - bb'b'' + ab'a'' + ba'a'') \qquad (1)$$
$$z\,.\,(z'\,.\,z'') = (a\,,b)\,[(a'\,,b')\,.\,(a''\,,b'')] = (a\,,b)\,(a'a'' - b'b''\,,a'b'' + b'a'') =$$
$$= (aa'a'' - ab'b'' - ba'b'' - bb'a''\,,aa'b'' + ab'a'' + ba'a'' - bb'b'') \qquad (2)$$

De (1) y (2) resulta

$$(zz')\,z'' = z\,(z'z'')$$

$G_3$ : Elemento neutro es el complejo $(1\,,0)$. En efecto, si $z = (x\,,y)$ es neutro para el producto, debe satisfacer

$$(a\,,b)\,.\,(x\,,y) = (x\,,y)\,.\,(a\,,b) = (a\,,b) \qquad \forall\,(a\,,b) \in \mathbf{C}$$

Por definición de multiplicación

$$(ax - by\ ,\ ay + bx) = (a\ ,\ b)$$

Por igualdad de complejos

$$\begin{cases} ax - by = a \\ bx + ay = b \end{cases}$$

Resolviendo el sistema

$$\Delta = \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 = \Delta\, x$$

$$\Delta\, y = \begin{vmatrix} a & a \\ b & b \end{vmatrix} = ab - ab = 0$$

Si $(a\ ,\ b) \neq (0\ ,\ 0)$ entonces

$$x = \frac{\Delta x}{\Delta} = 1 \ \wedge\ y = \frac{\Delta y}{\Delta} = 0$$

Resulta $(x\ ,\ y) = (1\ ,\ 0)$ que satisface $G_3$ para todo $(a\ ,\ b) \in C$, pues en el caso $(a\ ,\ b) = (0\ ,\ 0)$ se tiene

$$(0\ ,0)\ .\ (1\ ,\ 0) = (0\ .\ 1 - 0\ .\ 0\ ,\ 0\ .\ 0 + 0\ .\ 1) = (0\ ,0)$$

$G_4$ : Todo complejo no nulo admite inverso multiplicativo.
Sea $z = (a\ ,\ b) \neq (0\ ,\ 0)$. Si existe $z^{-1} = (x\ ,\ y)$, debe satisfacer

$$z\ .\ z^{-1} = z^{-1}\ .\ z = (1\ ,0)$$

Es decir

$$(a\ ,\ b)\ .\ (x\ ,y) = (x\ ,\ y)\ .\ (a\ ,\ b) = (1\ ,\ 0)$$

Efectuando el producto

$$(ax - by\ ,\ ay + bx) = (1\ ,\ 0)$$

Por igualdad de números complejos resulta el sistema

$$\begin{cases} ax - by = 1 \\ bx + ay = 0 \end{cases}$$

Resolviendo el sistema

$$\Delta = \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 \neq 0$$

$$\Delta x = \begin{vmatrix} 1 & -b \\ 0 & a \end{vmatrix} = a$$

$$\Delta y = \begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix} = -b$$

Luego

$$x = \frac{\Delta x}{\Delta} = \frac{a}{a^2+b^2} \quad \text{y} \quad y = \frac{\Delta y}{\Delta} = \frac{-b}{a^2+b^2}$$

O sea

$$z^{-1} = \left(\frac{a}{a^2+b^2} \ , \ -\frac{b}{a^2+b^2}\right)$$

$G_5$ : Conmutatividad.

$$z \,.\, z' = (a\,,b)\,.\,(a',b') = (aa' - bb'\,,\, ab' + ba') =$$
$$= (a'a - b'b\,,\, b'a + a'b) = (a'\,,b')\,(a\,,b) = z'z$$

de acuerdo con la definición de multiplicación en **C** y la conmutatividad del producto en **R**.

III) El producto es distributivo respecto de la suma. En efecto

$$(z+z')\,z'' = [(a\,,b) + (a',b')]\,(a'',b'') = (a+a',\, b+b')\,(a'',b'') =$$
$$= (aa'' + a'a'' - bb'' - b'b'',\, ab'' + a'b'' + ba'' + b'b'') =$$
$$= (aa'' - bb'',\, ab'' + ba'') + (a'a'' - b'b'',\, a'b'' + b'b'') =$$
$$= (a\,,b)\,.\,(a'',b'') + (a',b')\,(a'',b'') = zz'' + z'z''$$

Por adición en **C**, nultiplicación en **C** y conmutatividad de la suma en **R**.

En consecuencia, la terna (**C** , + , .) es un cuerpo. La diferencia esencial que presenta con relación al cuerpo de los números reales consiste en que es no ordenado. En efecto, si fuera ordenado, como $i \neq 0$, caben dos posibilidades:

$$i > 0 \quad \text{ó} \quad i < 0$$

En el primer caso, por la compatibilidad de la relación respecto del producto, se tiene $i^2 > 0$, es decir, $-1 > 0$, lo que es absurdo.

En el segundo caso es $0 < i$, y en consecuencia, $-i < 0$, y por la compatibilidad con el producto resulta $-i^2 < 0$, o sea, $1 < 0$, lo que también es absurdo.

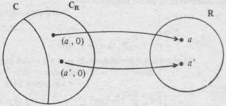
*Ejemplo 11-2.*

Sean $z_1 = (-2\,,3)$ , $z_2 = (1\,,2)$ y $z_3 = (-3\,,-1)$. Efectuar $(z_1 - z_2)\,.\,z_3$

$$(z_1 - z_2)\,z_3 = [(-2\,,3) - (1\,,2)]\,(-3\,,-1) =$$
$$= (-3\,,1)\,(-3\,,-1) = (9+1\,,3-3) = (10\,,0)$$

## 11.3. ISOMORFISMO DE LOS COMPLEJOS REALES EN LOS REALES

Sea $C_R = \{(a, b) \in C / b = 0\}$ el conjunto de los complejos de parte imaginaria nula. La función $f : C_R \to R$, definida por $f(a, 0) = a$, asigna a cada complejo real su primera componente.




La aplicación $f$ es obviamente biyectiva, y además un morfismo de $C_R$ en R respecto de la adición y multiplicación. En efecto, sean $z = (a, 0)$ y $z' = (a', 0)$; entonces

$$f(z + z') = f[(a, 0) + (a', 0)] = f(a + a' 0) =$$
$$= a + a' = f(a, 0) + f(a', 0) = f(z) + f(z')$$

Por otra parte

$$f(z z') = f[(a, 0)(a', 0)] = f(aa', 0) = aa' =$$
$$= f(a, 0) f(a', 0) = f(z) f(z')$$

En consecuencia, $f$ es un isomorfismo de $C_R$ en R respecto de la adición y multiplicación; o sea, $C_R$ y R son conjuntos indistinguibles desde el punto de vista algebraico.

El isomorfismo permite identificar cada complejo real con el real correspondiente, es decir, $(a, 0) = a$.

## 11.4. FORMA BINOMICA DE UN COMPLEJO

### 11.4.1. Unidad imaginaria

El número complejo imaginario de segunda componente igual a 1, se llama unidad imaginaria y se denota por

$$i = (0, 1)$$

La multiplicación de un complejo real por la unidad imaginaria permuta las componentes de aquél, es decir, lo trasforma en un complejo imaginario. En efecto

$$(b\,,0)\,.\,i=(b\,,0)\,.\,(0\,,1)=(b\,.\,0-0\,.\,1\,,b\,.\,1+0\,.\,0)=(0\,,b)$$

y por el isomorfismo de los complejos reales con los reales, se tiene

$$bi=(0\,,b)$$

Las potencias sucesivas de la unidad imaginaria son

$$i^0=1$$
$$i^1=i$$
$$i^2=(0\,,1)\,.\,(0\,,1)=(-1\,,0)=-1$$
$$i^3=i^2\,.\,i=(-1)\,.\,i=-i$$

Análogamente

$$i^4=1 \qquad i^5=i \qquad i^6=-1 \qquad i^7=-i$$

Si el exponente es de la forma $4\,k$ con $k \in \mathbf{Z}$, se tiene $i^{4k}=(i^4)^k=1^k=1$

En general, si el exponente de $i$ es $a \in \mathbf{N}$, al efectuar la división por 4 se tiene $a=4\,q+r$, donde $0 \leqslant r < 4$. En consecuencia

$$i^a=i^{4q+r}=i^{4q}\,.\,i^r=1\,.\,i^r=i^r$$

y este cálculo se reduce a uno de los cuatro considerados en primer término.

### 11.4.2. Forma binómica de los complejos

Sea $z=(a\,,b)$ un número complejo.

Por definición de suma

$$z=(a\,,0)+(0\,,b)$$

Por el isomorfismo de los complejos reales con los reales, y por 11.4.1, resulta la forma binómica

$$z=a+bi$$

La conveniencia de la forma binómica se pone de manifiesto al efectuar operaciones con números complejos, evitando el cálculo con pares ordenados, que es más laborioso.

*Ejemplo 11-3.*

Sean $z_1=(-2\,,3)$ , $z_2=(1\,,2)$ y $z_3=(-3\,,1)$. Calcular $(z_1-z_2)\,z_3^2$

Con la representación binómica se tiene

$$
\begin{aligned}
(z_1 - z_2)\, z_3^2 &= [(-2 + 3i) - (1 + 2i)](-3 + i)^2 = \\
&= (-3 + i)(9 + i^2 - 6i) = (-3 + i)(9 - 1 - 6i) = \\
&= (-3 + i)(8 - 6i) = -24 + 18i + 8i - 6i^2 = \\
&= -24 + 26i + 6 = -18 + 26i
\end{aligned}
$$

## 11.5. LA CONJUGACION EN C

### 11.5.1. Complejos conjugados

Sea $z = a + bi$.

***Definición***

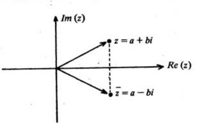
Conjugado de $z = a + bi$ es el número complejo $\bar{z} = a - bi$.
El símbolo $\bar{z}$ se lee "conjugado de $z$" o "$z$ conjugado".
Si $z = -1 + 3i$, entonces $\bar{z} = -1 - 3i$.
El conjugado de $z = \left(\frac{3}{2}, -1\right)$ es $\bar{z} = \left(\frac{3}{2}, 1\right)$.

Dado $z = a + bi$ se tiene $\bar{z} = a - bi$ y $\bar{\bar{z}} = a + bi = z$, es decir, que el conjugado del conjugado de un número complejo es igual a éste. Los complejos $z$ y $\bar{z}$ se llaman conjugados.

***Definición***

Dos complejos son conjugados si y sólo si tienen la misma parte real, y sus partes imaginarias son números opuestos.

Dos complejos conjugados caracterizan puntos simétricos respecto del eje real.




**11.5.2. Propiedad** La suma de dos complejos conjugados es igual al duplo de la parte real. El producto de dos complejos conjugados es un número real no negativo.

En efecto, sea $z = a + bi$. Entonces

$$z + \bar{z} = (a + bi) + (a - bi) = 2a = 2\,Re\,(z)$$

Por otra parte

$$z \cdot \overline{z} = (a+bi) \cdot (a-bi) = a^2 - (bi)^2 = a^2 + b^2$$

Como $a$ y $b$ son números reales, resulta

$$z \cdot \overline{z} \in \mathbf{R} \ \wedge \ z \cdot \overline{z} \geqslant 0$$

**11.5.3. Propiedad.** Un número complejo es real si y sólo si es igual a su conjugado.

$$z \in \mathbf{R} \Leftrightarrow z = \overline{z}$$

i ) $z \in \mathbf{R} \Rightarrow z = a + 0i \Rightarrow z = a \ \wedge \ \overline{z} = a \Rightarrow z = \overline{z}$

ii ) $z = \overline{z} \Rightarrow a + bi = a - bi \Rightarrow bi = -bi \Rightarrow 2bi = 0 \Rightarrow b = 0$

Entonces $z = a$, o lo que es lo mismo, $z \in \mathbf{R}$

**11.5.4. Automorfismo en C**

La función $f : \mathbf{C} \to \mathbf{C}$ definida por $f(z) = \overline{z}$ es un automorfismo en **C**. En efecto

i ) $f$ es inyectiva. Sean $z$ y $z'$ en **C**, tales que $f(z) = f(z')$

$$f(z) = f(z') \Rightarrow \overline{z} = \overline{z'} \Rightarrow a - bi = a' - b'i$$

y por igualdad de complejos resulta $a = a' \ \wedge \ b = b'$, o sea $z = z'$.

ii ) $f$ es sobreyectiva. Para todo $w = a + bi \in \mathbf{C}$, existe $z = a - bi$, tal que

$$f(z) = f(a - bi) = a + bi = w$$

iii) $f$ es un morfismo respecto de la adición, pues

$$\begin{aligned} f(z+z') &= \overline{z+z'} = \\ &= \overline{(a+bi)+(a'+b'i)} = \overline{(a+a')+(b+b')i} = \\ &= (a+a') - (b+b')i = (a-bi) + (a'-b'i) = \\ &= \overline{z} + \overline{z'} = f(z) + f(z') \end{aligned}$$

Por definición de $f$ y suma en **C**.

iv) $f$ es un morfismo respecto de la multiplicación, ya que

$$\begin{aligned} f(zz') &= \overline{zz'} = \overline{(a+bi)(a'+b'i)} = \\ &= \overline{(aa'-bb')+(ab'+ba')i} = (aa'-bb') - (ab'+ba')i = \\ &= (a-bi)(a'-b'i) = \overline{z}\,\overline{z'} = f(z)f(z') \end{aligned}$$

Las propiedades iii) y iv) se traducen en el siguiente enunciado: "el conjugado de la suma es igual a la suma de los conjugados, y el conjugado del producto es igual al producto de los conjugados".

$$\overline{z+z'} = \overline{z} + \overline{z'}$$

$$\overline{zz'} = \overline{z}\,\overline{z'}$$

*Ejemplo 11-4.*

Determinar los complejos $z = x + yi$ que satisfacen

i ) $z = -\bar{z}$

En la forma binómica se tiene

$$x + yi = -(x - yi) \Rightarrow x + yi = -x + yi \Rightarrow x = -x \Rightarrow x = 0$$

Los complejos que verifican la condición dada son de la forma $z = yi$, es decir, imaginarios puros, y corresponden al eje de ordenadas.

ii ) $z \cdot \bar{z} = 1$

Esta condición se traduce en

$$(x + yi) \cdot (x - yi) = 1$$

Luego, $x^2 + y^2 = 1$, y corresponde a la circunferencia de radio 1 con centro en el origen.

## 11.6. MODULO DE UN COMPLEJO

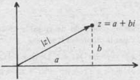
**11.6.1.** Sea $z = a + bi$.

***Definición***

Módulo de un complejo es la raíz cuadrada no negativa de la suma de los cuadrados de las partes real e imaginaria.

La notación es $|z| = \sqrt{a^2 + b^2}$.

El módulo de un complejo es la distancia del punto correspondiente, al origen.




Si $z = -3 + 4i$, entonces $|z| = \sqrt{(-3)^2 + 4^2} = \sqrt{25} = 5$.

**11.6.2. Propiedades del módulo**

I) El módulo de todo complejo es mayor o igual que su parte real

Sea $z = a + bi$. Entonces

$$|a|^2 = a^2 \Rightarrow |a|^2 \leqslant a^2 + b^2 \Rightarrow |a|^2 \leqslant |z|^2 \Rightarrow |a| \leqslant |z|$$

Como $a \in \mathbf{R} \Rightarrow a \leqslant |a|$, de esta relación y de $|a| \leqslant |z|$ resulta $|z| \geqslant a$, es decir, $Re\,(z) \leqslant |z|$.

Análogamente $Im\,(z) \leqslant |z|$

II) El producto de cualquier complejo por su conjugado es igual al cuadrado del módulo.

Tesis) $z\,.\,\bar{z} = |z|^2$

Demostración)

Efectuando el producto y aplicando la definición de módulo, resulta

$$z\,.\,\bar{z} = (a + bi)\,.\,(a - bi) = a^2 - (bi)^2 = a^2 + b^2 = |z|^2$$

III) El módulo del producto de dos complejos es igual al producto de los módulos.

Tesis) $|z\,z'| = |z|\,|z'|$

Demostración)

A partir del cuadrado del primer miembro aplicamos II, conjugado del producto, conmutatividad y asociatividad del producto en **C** y la propiedad II

$$|zz'|^2 = zz'\overline{zz'} = zz'\bar{z}\bar{z'} = z\bar{z}z'\bar{z'} =$$
$$= |z|^2\,|z'|^2$$

Resulta

$$|zz'|^2 = (|z|\,|z'|)^2$$

Y como las bases son no negativas, se tiene

$$|zz'| = |z|\,|z'|$$

IV) El módulo de la suma de dos complejos es menor o igual que la suma de los módulos.

Tesis) $|z + z'| \leqslant |z| + |z'|$

Demostración)

Por cuadrado del módulo, conjugado de la suma, distributividad del producto respecto de la suma en **C** y por la propiedad **II** se tiene

$$|z + z'|^2 = (z + z')\,(\overline{z + z'}) = (z + z')\,(\bar{z} + \bar{z'}) =$$
$$= z\bar{z} + z\bar{z'} + z'\bar{z} + z'\bar{z'} = |z|^2 + z\bar{z'} + \bar{z}z' + |z'|^2$$

$$\overline{\bar{z}z'} = \bar{\bar{z}}\,\bar{z'} = z\bar{z'}$$

Como los términos centrales son complejos conjugados, su suma es el duplo de la parte real, es decir

$$z\bar{z'} + \bar{z}z' = 2\,Re\,(z\bar{z'})$$

Sustituyendo en la igualdad inicial tenemos

$$|z + z'|^2 = |z|^2 + 2\,Re\,(z\bar{z'}) + |z'|^2 \qquad (1)$$

Ahora bien, teniendo en cuenta que la parte real es menor o igual que el módulo

$$2\, Re\, (z\overline{z'}) \leqslant 2\, |z\overline{z'}|$$

Por módulo del producto

$$2\, Re\, (z\overline{z'}) \leqslant 2\, |z|\, |\overline{z'}|$$

y como $|\overline{z}'| = |z'|$, es

$$2\, Re\, (z\overline{z'}) \leqslant 2\, |z|\, |z'| \qquad (2)$$

Sumando (1) y (2)

$$|z + z'|^2 + 2\, Re\, (z\overline{z'}) \leqslant |z|^2 + 2\, Re\, (z\overline{z'}) + |z'|^2 + 2\, |z|\, |z'|$$

Después de cancelar y factorear el segundo miembro

$$|z + z'|^2 \leqslant (|z| + |z'|)^2$$

y como las bases son no negativas, resulta

$$|z + z'| \leqslant |z| + |z'|$$

V) El módulo de una potencia de exponente natural es igual a la potencia del módulo

$$|z^n| = |\underbrace{z \cdot z \ldots z}_{n}| = \underbrace{|z|\, |z| \ldots |z|}_{n} = |z|^n$$

*Ejemplo 11-5.*

Al dividir dos complejos, siendo el segundo distinto de cero, puede evitarse la determinación del inverso multiplicativo del divisor multiplicando por el conjugado de éste, y se obtiene

$$\frac{z}{w} = \frac{z\,\overline{w}}{w\,\overline{w}} = \frac{z\,\overline{w}}{|w|^2}$$

En particular

$$\frac{-1+2i}{2+3i} = \frac{(-1+2i)(2-3i)}{(2+3i)(2-3i)} = \frac{-2+3i+4i-6i^2}{2^2+3^2} =$$

$$= \frac{-2+7i+6}{13} = \frac{4+7i}{13} = \frac{4}{13} + \frac{7}{13}\, i$$

*Ejemplo 11-6.*

Determinar los complejos $z$ que satisfacen

i ) $iz = 1 + i$

$$z = \frac{1+i}{i} = \frac{(1+i)(-i)}{i(-i)} = \frac{-i-i^2}{1} =$$

$$= -i + 1 = 1 - i$$

ii) $|z-1+2i|=2$

Si $z=x+yi$, entonces

$$|x+yi-1+2i|=2 \Rightarrow$$
$$\Rightarrow |(x-1)+(y+2)i|=2 \Rightarrow$$
$$\Rightarrow \sqrt{(x-1)^2+(y+2)^2}=2 \Rightarrow$$
$$\Rightarrow (x-1)^2+(y+2)^2=4$$

Es la ecuación de la circunferencia de radio 2, con centro $(1\,,-2)$.

iii)

$$|z-Re\,(z)|=[Im\,(z)]^2$$
$$z=x+yi \Rightarrow |x+yi-x|=y^2 \Rightarrow$$
$$\Rightarrow |yi|=y^2 \Rightarrow (\sqrt{y^2})^2=y^2 \Rightarrow$$
$$\Rightarrow |y|=y^2 \Rightarrow y^2=y \text{ con } y\geqslant 0 \Rightarrow$$
$$\Rightarrow y^2-y=0 \Rightarrow y\,(y-1)=0 \Rightarrow$$
$$\Rightarrow y=0 \ \vee\ y=1 \Rightarrow z=x \ \vee\ z=x+i$$

Se obtienen los complejos correspondientes a los puntos de las rectas de ecuaciones $y=0 \vee y=1$.

iv) $z=-\bar{z}+2$

$$z=x+yi \Rightarrow z+\bar{z}=2 \Rightarrow$$
$$\Rightarrow 2x=2 \Rightarrow x=1 \Rightarrow z=1$$

Es la recta de ecuación $x=1$

v) $(a+bi)\,z=(a^2+b^2)\,i$ con $(a\,,b)\neq(0\,,0)$

Se tiene

$$z=\frac{(a^2+b^2)\,i}{a+bi}=\frac{(a^2+b^2)\,i\,(a-bi)}{(a+bi)\,(a-bi)}=$$
$$=\frac{(a^2+b^2)\,i\,(a-bi)}{a^2+b^2}=i\,(a-bi)=ai-bi^2=$$
$$=b+ai$$

## 11.7. RAIZ CUADRADA EN C

Sea $z=a+bi$. Por definición, la raíz cuadrada de $z$ es un complejo $x+yi$ que satisface

$$(x+yi)^2=a+bi \qquad (1)$$

Aplicando módulos

$$|(x+yi)^2|=|a+bi|$$

Por 11.6.2. v) y por definición de módulo

$$|x + yi|^2 = \sqrt{a^2 + b^2}$$

Por cuadrado del módulo

$$x^2 + y^2 = \sqrt{a^2 + b^2}$$

Es decir

$$x^2 + y^2 = |z| \qquad (2)$$

Desarrollando (1)

$$x^2 - y^2 + 2\,xyi = a + bi$$

Por igualdad de complejos

$$x^2 - y^2 = a \qquad (3)$$

$$2\,xy = b \qquad (4)$$

Sumando y restando (2) y (3)

$$\begin{cases} x^2 + y^2 = |z| \\ x^2 - y^2 = a \end{cases}$$

$$2\,x^2 = |z| + a$$

$$2\,y^2 = |z| - a$$

Resulta

$$x = \pm\sqrt{\frac{|z| + a}{2}}$$

$$y = \pm\sqrt{\frac{|z| - a}{2}}$$

Ambos radicandos son no negativos, pues $|z| \geqslant a$, y se obtienen cuatro pares de valores reales, de los cuales se seleccionan dos de acuerdo con la condición (4): si $b > 0$, entonces $x$ e $y$ se eligen con el mismo signo, y si $b < 0$, se eligen con distinto signo.

***Ejemplo 11-7.***

Calcular las raíces cuadradas de los siguientes complejos

i ) $z = -4 - 3\,i$

$$a = -4\,,\, b = -3\,,\, |z| = 5$$

$$x = \pm\sqrt{\frac{5-4}{2}} = \pm\frac{1}{\sqrt{2}} = \pm\frac{\sqrt{2}}{2}$$

$$y = \pm\sqrt{\frac{5+4}{2}} = \pm\frac{3}{\sqrt{2}} = \pm\frac{3\sqrt{2}}{2}$$

Como $b < 0$, $x$ e $y$ se eligen con signos distintos, y las soluciones son

$$\left(\frac{\sqrt{2}}{2}, \frac{-3\sqrt{2}}{2}\right), \left(-\frac{\sqrt{2}}{2}, \frac{3\sqrt{2}}{2}\right)$$

Es decir

$$\sqrt{-4-3i} = \pm\left(\frac{\sqrt{2}}{2} - \frac{3\sqrt{2}}{2}i\right)$$

ii) $z = -2i$

$a = 0$, $b = -2$, $|z| = 2$

$$x = \pm\sqrt{\frac{2+0}{2}} = \pm 1 = y$$

Como $b = -2 < 0$, las soluciones son

$$(1, -1) \quad \text{y} \quad (-1, 1)$$

Luego

$$\sqrt{-2i} = \pm(1 - i)$$

iii) $z = -9$

$a = -9$, $b = 0$, $|z| = 9$

$$x = \pm\sqrt{\frac{9-9}{2}} = 0$$

$$y = \pm\sqrt{\frac{9+9}{2}} = \pm 3$$

En este caso, los cuatro pares de valores se reducen a dos

$$(0, 3) \quad \text{y} \quad (0, -3)$$

y se tiene

$$\sqrt{-9} = \sqrt{-9+0i} = \pm(0+3i) = \pm 3i$$

Análogamente

$$\sqrt{-\frac{1}{4}} = \pm\frac{1}{2}i$$

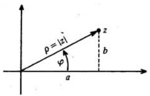
$$\sqrt{-3} = \pm\sqrt{3}\,i$$

## 11.8. FORMA POLAR O TRIGONOMETRICA

Sea $z = a + bi$ un complejo no nulo. Las coordenadas polares del punto de coordenadas cartesianas $a$ y $b$ son: el radio vector $\rho$ y el argumento $\varphi$, o cualquiera de los congruentes a $\varphi$, módulo $2\pi$.

Las fórmulas de pasaje de las coordenadas polares a cartesianas son

$$a = \rho \cos \varphi$$
$$b = \rho \operatorname{sen} \varphi$$




donde $\rho = \sqrt{a^2 + b^2} = |z|$ y $\varphi = \arg z$

Se tiene

$$z = a + bi = \rho \cos \varphi + \rho\, i \operatorname{sen} \varphi$$

es decir

$$z = \rho (\cos \varphi + i \operatorname{sen} \varphi)$$

Esta es la llamada forma polar o trigonométrica del complejo $z$.

Es claro que $\rho$ y $\varphi$ definen unívocamente a $z$. Pero $z$ caracteriza unívocamente a $\rho$, y no a $\varphi = \arg z$.

***Definición***

Argumento principal del complejo no nulo $z$ es el número real $\varphi$ que satisface

i ) $a = |z| \cos \varphi \;\wedge\; b = |z| \operatorname{sen} \varphi$

ii ) $0 \leqslant \varphi < 2\pi$

Para denotar el argumento principal escribiremos $\varphi = \operatorname{Arg} z$.

Dados dos complejos en forma polar $z = \rho (\cos \rho + i \operatorname{sen} \varphi)$ y $z' = \rho' (\cos \varphi, + i \operatorname{sen} \varphi')$ diremos que son iguales si y sólo si tienen el mismo módulo y sus argumentos son congruentes módulo $2\pi$. En símbolos

$$z = z' \Leftrightarrow \rho = \rho' \;\wedge\; \varphi' = \varphi + 2k\pi \quad \text{con } k \in \mathbf{Z}$$

***Ejemplo 11-8.***

Determinar la forma polar de los siguientes complejos

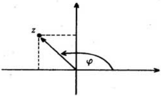
i ) $z = -2 + 2i$

$$\rho = \sqrt{(-2)^2 + 2^2} = \sqrt{8} = 2\sqrt{2}$$

Para el argumento principal consideramos

$$\cos \varphi = \frac{a}{\rho} = \frac{-2}{2\sqrt{2}} = -\frac{\sqrt{2}}{2}$$

$$\operatorname{sen} \varphi = \frac{b}{\rho} = \frac{2}{2\sqrt{2}} = \frac{\sqrt{2}}{2}$$



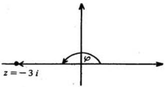

Resulta $\varphi$ del segundo cuadrante e igual a 135°.
Luego $z = 2\sqrt{2}\,(\cos 135° + i \operatorname{sen} 135°)$

ii) $z = -3i$

$\rho = \sqrt{0^2 + (-3)^2} = 3$

$\varphi = \pi$

Luego $z = 3\,(\cos \pi + i \operatorname{sen} \pi)$




## 11.9 OPERACIONES EN FORMA POLAR

### 11.9.1. Multiplicación

El producto de dos complejos en forma polar tiene por módulo el producto de los módulos, y por argumento la suma de los argumentos.

Sean $z = \rho\,(\cos \varphi + i \operatorname{sen} \varphi)$ y $z' = \rho'\,(\cos \varphi' + i \operatorname{sen} \varphi')$

Entonces

$$zz' = \rho\rho' (\cos\varphi + i \operatorname{sen}\varphi)(\cos\varphi' + i \operatorname{sen}\varphi') =$$
$$= \rho\rho' [(\cos\varphi\cos\varphi' - \operatorname{sen}\varphi\operatorname{sen}\varphi') + i(\operatorname{sen}\varphi\cos\varphi' + \cos\varphi\operatorname{sen}\varphi')]$$
$$= \rho\rho' [\cos(\varphi + \varphi') + i \operatorname{sen}(\varphi + \varphi')]$$

### 11.9.2. Cociente

El cociente de dos complejos en forma polar, siendo el segundo distinto de cero, tiene por módulo el cociente de los módulos, y por argumento la diferencia de los argumentos.

$$\frac{z}{z'} = w \Rightarrow z = z'w \Rightarrow$$
$$\Rightarrow \rho(\cos\varphi + i \operatorname{sen}\varphi) = \rho' (\cos\varphi' + i \operatorname{sen}\varphi')\, \mathrm{R}(\cos\phi + i \operatorname{sen}\phi) \Rightarrow$$
$$\Rightarrow \rho(\cos\varphi + i \operatorname{sen}\varphi) = \mathrm{R}\,\rho' [\cos(\phi + \varphi') + i \operatorname{sen}(\phi + \varphi')]$$

Por igualdad de complejos

$$\mathrm{R}\,\rho' = \rho \;\wedge\; \phi + \varphi' = \varphi + 2k\pi$$

Luego

$$\mathrm{R} = \frac{\rho}{\rho'} \;\wedge\; \phi = \varphi - \varphi' \quad \text{si} \quad k = 0$$

$$\Rightarrow \frac{z}{z'} = \frac{\rho}{\rho'} [\cos(\varphi - \varphi') + i \operatorname{sen}(\varphi - \varphi')]$$

### 11.9.3. Potenciación de exponente natural

La potencia $n$-sima de un complejo en forma polar tiene por módulo la potencia $n$-sima de su módulo, y por argumento el producto de su argumento por $n$.

$$z = \rho(\cos\varphi + i \operatorname{sen}\varphi) \Rightarrow z^n = \rho^n (\cos n\varphi + i \operatorname{sen} n\varphi)$$

Lo demostramos por inducción completa

1º) $n = 1 \Rightarrow z^1 = z = \rho(\cos\varphi + i \operatorname{sen}\varphi) =$
$= \rho^1 (\cos 1 \,.\, \varphi + i \operatorname{sen} 1 \,.\, \varphi)$

2º) $z^h = \rho^h (\cos h\varphi + i \operatorname{sen} h\varphi) \Rightarrow z^{h+1} = \rho^{h+1} [\cos(h+1)\varphi + i \operatorname{sen}(h+1)\varphi]$

En efecto, por definición de potencia, hipótesis inductiva y 11.9.1., se tiene

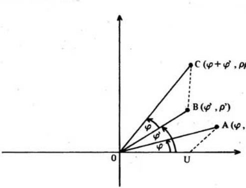
$$z^{h+1} = z^h z = \rho^h (\cos h\varphi + i \operatorname{sen} h\varphi)\, \rho(\cos\varphi + i \operatorname{sen}\varphi) =$$
$$= \rho^{h+1} [\cos(h+1)\varphi + i \operatorname{sen}(h+1)\varphi]$$

La fórmula $z^n = \rho^n (\cos n\varphi + i \operatorname{sen} n\varphi)$ se llama de De Moivre.

### 11.9.4. Determinación geométrica del producto y del cociente

Sean $z = \rho (\cos \varphi + i \operatorname{sen} \varphi)$ y $z' = \rho' (\cos \varphi' + i \operatorname{sen} \varphi')$.

i ) *Producto.* En un sistema cartesiano consideramos U (1 , 0) y los puntos A y B representantes de los complejos $z$ y $z'$, es decir, de coordenadas polares $(\varphi , \rho)$ y $(\varphi' , \rho')$, respectivamente.




Considerando a OB como homólogo de OU, construimos $O\hat{B}C \sim O\hat{U}A$. Resulta C de coordenadas polares $(\varphi + \varphi' , R)$, y por la proporcionalidad de lados homólogos

$$\frac{d(0, C)}{d(0, A)} = \frac{d(0, B)}{d(0, U)}$$

es decir

$$\frac{R}{\rho} = \frac{\rho'}{1} \Rightarrow R = \rho\rho'$$

En consecuencia, el vector $\overrightarrow{OC}$ representa el producto de los complejos $z$ y $z'$.

ii ) *Cociente.* Razonando sobre la misma figura, suponemos dados los puntos C y B asociados al dividendo y divisor respectivamente. Construimos sobre OU, como homólogo de OB, el triángulo $O\hat{U}A$ semejante a $O\hat{B}C$, y obtenemos el vector $\overrightarrow{OA}$, es decir, el cociente.

*Ejemplo 11-9.*

Siendo $z = -1 + i\sqrt{3}$ y $z' = \frac{3}{2} + \frac{3\sqrt{3}}{2}\,i$; realizar en forma polar las siguientes operaciones

$$z \,.\, z' \,, \quad \frac{z}{z'} \,, \quad z^6$$

Expresamos $z$ y $z'$ en forma polar

$$\rho = \sqrt{(-1)^2 + (\sqrt{3})^2} = \sqrt{4} = 2$$

$\operatorname{sen} \varphi = \frac{b}{\rho} = \frac{\sqrt{3}}{2} \Rightarrow \varphi = 120°$ pues $z$ caracteriza un punto del segundo cuadrante.

Luego

$$z = 2\,(\cos 120° + i \operatorname{sen} 120°)$$

Por otra parte

$$\rho' = \sqrt{\left(\frac{3}{2}\right)^2 + \left(\frac{3\sqrt{3}}{2}\right)^2} = \sqrt{\frac{9}{4} + \frac{27}{4}} = \sqrt{\frac{36}{4}} = 3$$

$\operatorname{sen} \varphi' = \frac{b}{\rho} = \frac{\sqrt{3}}{2} \Rightarrow \varphi = 60°$, ya que $z'$ corresponde a un punto del primer cuadrante.

Entonces

$$z' = 3\,(\cos 60° + i \operatorname{sen} 60°)$$

Aplicando las fórmulas deducidas tenemos

i ) $zz' = 6\,(\cos 180° + i \operatorname{sen} 180°) = 6\,(-1 + 0\,i) = -6$

ii ) $\frac{z}{z'} = \frac{2}{3}\,(\cos 60° + i \operatorname{sen} 60°) =$

$$= \frac{2}{3}\left(\frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right) = \frac{1}{3} + \frac{\sqrt{3}}{3}\,i$$

iii) $z^6 = 2^6\,(\cos 6\,.\,120° + i \operatorname{sen} 6\,.\,120°) = 2^6\,(\cos 720° + i \operatorname{sen} 720°) =$

$$= 2^6\,(\cos 0° + i \operatorname{sen} 0°) = 2^6\,(1 + 0\,.\,i) = 2^6 = 64$$

*Ejemplo 11-10.*

Mediante la fórmula de De Moivre, obtener $\operatorname{sen} 2\varphi$ y $\cos 2\varphi$.

Sea $z$ un complejo de módulo 1 y argumento $\varphi$, es decir

$$z = \cos \varphi + i \operatorname{sen} \varphi$$

Elevamos al cuadrado de dos maneras: por cuadrado de un binomio

$$z^2 = (\cos\varphi + i \operatorname{sen}\varphi)^2 = \cos^2\varphi - \operatorname{sen}^2\varphi + 2\,i \operatorname{sen}\varphi\cos\varphi \qquad (1)$$

y por la fórmula de De Moivre

$$z^2 = (\cos\varphi + i \operatorname{sen}\varphi)^2 = \cos 2\varphi + i \operatorname{sen} 2\varphi \qquad (2)$$

De (1) y (2) resulta

$$\cos 2\varphi = \cos^2\varphi - \operatorname{sen}^2\varphi$$

$$\operatorname{sen} 2\varphi = 2 \operatorname{sen}\varphi\cos\varphi$$

## 11.10. RADICACION EN C

Por definición, el complejo $w$ es raíz $n$-sima de $z$ si y sólo si $z^n = w$.

**Teorema.** Todo complejo no nulo admite $n$ raíces $n$-simas distintas dadas por

$$w_k = \sqrt[n]{\rho}\left(\cos\frac{\varphi + 2\,k\,\pi}{n} + i \operatorname{sen}\frac{\varphi + 2\,k\,\pi}{n}\right)$$

donde $k = 0, 1, 2, \ldots, n-1$ , $\rho = |z|$ y $\varphi = \arg z$

Demostración)

Sean $z = \rho\,(\cos\varphi + i \operatorname{sen}\varphi)$ y $w = R\,(\cos\Phi + i \operatorname{sen}\Phi)$

Por definición de raíz, debe ser

$$w^n = z$$

Es decir

$$R^n\,(\cos n\,\Phi + i \operatorname{sen} n\,\Phi) = \rho\,(\cos\varphi + i \operatorname{sen}\varphi)$$

Por igualdad de complejos

$$R^n = \rho \quad \text{y} \quad n\,\Phi = \varphi + 2\,k\,\pi$$

Luego

$$R = \sqrt[n]{\rho} \quad \text{y} \quad \Phi = \frac{\varphi + 2\,k\,\pi}{n}$$

Se obtiene la fórmula

$$\sqrt[n]{\rho\,(\cos\varphi + i \operatorname{sen}\varphi)} = \sqrt[n]{\rho}\left(\cos\frac{\varphi + 2\,k\,\pi}{n} + i \operatorname{sen}\frac{\varphi + 2\,k\,\pi}{n}\right)$$

Todas las raíces de $z$ tienen el mismo módulo, y difieren en el argumento que es

$$\frac{\varphi}{n} + \frac{2\,k\,\pi}{n} \qquad \text{con } k \in Z$$

De los infinitos valores enteros de $k$ es suficiente considerar $0, 1, 2, \ldots, n-1$ para obtener las $n$ raíces distintas.

| RAICES | ARGUMENTOS |
|---|---|
| $w_0$ | $\frac{\varphi}{n}$ |
| $w_1$ | $\frac{\varphi}{n} + \frac{2\pi}{n}$ |
| $w_2$ | $\frac{\varphi}{n} + 2 \, . \, \frac{2\pi}{n}$ |
| $w_3$ | $\frac{\varphi}{n} + 3 \, . \, \frac{2\pi}{n}$ |
| ... | ............... |
| $w_{n-1}$ | $\frac{\varphi}{n} + (n-1) \frac{2\pi}{n}$ |

Si $k = n$ entonces la correspondiente raíz $w_n$ tiene argumento

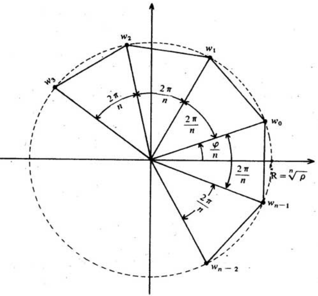
$$\frac{\varphi}{n} + n \, \frac{2\pi}{n} = \frac{\varphi}{n} + 2\pi$$

Que es congruente a $\frac{\varphi}{n}$ y se vuelve a obtener $w_0$.

En general $w_{j+n} = w_j$ y sólo existen $n$ raíces distintas.

*Nota*

Las $n$ raíces $n$-simas, distintas de un complejo no nulo, se identifican con los vértices de un polígono regular de $n$ lados inscripto en la circunferencia de radio $R = \sqrt[n]{\rho}$.




***Ejemplo 11-11.***

Calcular y representar

i ) $\sqrt[4]{-4+4i\sqrt{3}}$

$$z = -4 + 4i\sqrt{3} \Rightarrow \rho = \sqrt{(-4)^2 + (4\sqrt{3})^2} = \sqrt{64} = 8$$

$$\cos\varphi = \frac{a}{\rho} = \frac{-4}{8} = \frac{-1}{2} \Rightarrow \varphi = 120^\circ = \frac{2\pi}{3}$$

pues $z$ corresponde a un punto del segundo cuadrante.

El argumento de $w_k$ es

$$\Phi_k = \frac{\frac{2\pi}{3} + 2k\pi}{4} = \frac{\pi}{6} + \frac{k\pi}{2}$$

y se tienen los cuatro argumentos ·

$$\Phi_0 = \frac{\pi}{6} = 30^o$$

$$\Phi_1 = \frac{\pi}{6} + \frac{\pi}{2} = 30^o + 90^o = 120^o$$

$$\Phi_2 = \frac{\pi}{6} + \pi = 30^o + 180^o = 210^o$$

$$\Phi_3 = \frac{\pi}{6} + 3\ \frac{\pi}{2} = 30^o + 270^o = 300^o$$

Las cuatro raíces son

$$w_0 = \sqrt[4]{8}\,(\cos 30^o + i \text{ sen } 30^o) = \sqrt[4]{8}\left(\frac{\sqrt{3}}{2} + \frac{1}{2}\, i\right)$$

$$w_1 = \sqrt[4]{8}\,(\cos 120^o + i \text{ sen } 120^o) =$$

$$= \sqrt[4]{8}\,(-\cos 60^o + i \text{ sen } 60^o) = \sqrt[4]{8}\left(-\frac{1}{2} + i\ \frac{\sqrt{3}}{2}\right)$$

$$w_2 = \sqrt[4]{8}\,(\cos 210^o + i \text{ sen } 210^o) =$$

$$= \sqrt[4]{8}\,(-\cos 30^o - i \text{ sen } 30^o) = \sqrt[4]{8}\left(-\frac{\sqrt{3}}{2} - \frac{1}{2}\, i\right)$$

$$w_3 = \sqrt[4]{8}\,(\cos 300^o + i \text{ sen } 300^o) =$$

$$= \sqrt[4]{8}\,(\cos 60^o - i \text{ sen } 60^o) = \sqrt[4]{8}\left(\frac{1}{2} - i\ \frac{\sqrt{3}}{2}\right)$$

ii) $\sqrt[3]{1}$

$$z = 1 + 0\, i \Rightarrow \rho = 1 \ \wedge\ \varphi = 0$$

$$\Rightarrow \sqrt[3]{1\,(\cos 0 + i \text{ sen } 0)} = \sqrt[3]{1}\left(\cos\ \frac{0 + 2\, k\, \pi}{3} + i \text{ sen }\ \frac{0 + 2\, k\, \pi}{3}\right) =$$

$$= \cos\ \frac{2\, k\, \pi}{3} + i \text{ sen }\ \frac{2\, k\, \pi}{3}$$

Entonces

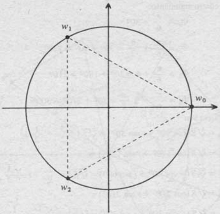
$$w_0 = \cos 0 + i \text{ sen } 0 = 1$$

$$w_1 = \cos\ \frac{2\,\pi}{3} + i \text{ sen }\ \frac{2\,\pi}{3} = \cos 120^o + i \text{ sen } 120^o =$$

$$= -\cos 60^o + i \text{ sen } 60^o = -\frac{1}{2} + i\ \frac{\sqrt{3}}{2}$$

$$w_2 = \cos\ \frac{4\,\pi}{3} + i \text{ sen }\ \frac{4\,\pi}{3} = \cos 240^o + i \text{ sen } 240^o =$$

$$= -\cos 60^o - i \text{ sen } 60^o = -\frac{1}{2} - i\ \frac{\sqrt{3}}{2}$$




## 11.11. FORMA EXPONENCIAL EN C

### 11.11.1. Exponencial compleja

En los cursos de Análisis se demuestra que la exponencial real $e^x$ admite el desarrollo en serie

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

y satisface las propiedades básicas $e^0 = 1$ y $e^x\, e^y = e^{x+y}$.

A fin de preservar estas propiedades definimos la exponencial compleja mediante

$$e^{ix} = \cos x + i \operatorname{sen} x$$

Se verifica

$$\begin{aligned} e^{ix} \,.\, e^{iy} &= (\cos x + i \operatorname{sen} x)(\cos y + i \operatorname{sen} y) = \\ &= (\cos x \cos y - \operatorname{sen} x \operatorname{sen} y) + i(\operatorname{sen} x \cos y + \cos x \operatorname{sen} y) = \\ &= \cos(x+y) + i \operatorname{sen}(x+y) = e^{i(x+y)} \end{aligned}$$

Sea $z = \rho\,(\cos\varphi + i \operatorname{sen}\varphi)$. Entonces $z = \rho\, e^{i\varphi}$ es la forma exponencial del complejo $z$.

### 11.11.2. Operaciones en forma exponencial

La traducción de las fórmulas relativas al producto, cociente y potenciación, obtenidas en la forma polar son las siguientes

i ) $z \cdot z' = \rho\, e^{i\varphi}\, \rho'\, e^{i\varphi'} = \rho\rho'\, e^{i(\varphi+\varphi')}$

ii ) $\dfrac{z}{z'} = \dfrac{\rho\, e^{i\varphi}}{\rho'\, e^{i\varphi'}} = \dfrac{\rho}{\rho'}\, e^{i(\varphi-\varphi')}$

iii) $z^n = (\rho\, e^{i\varphi})^n = \rho^n\, e^{in\varphi}$

*Ejemplo 11-12.*

Demostrar

i ) $z = e^{i\varphi} \Rightarrow |z| = 1$

En efecto

$$z = e^{i\varphi} \Rightarrow z = \cos\varphi + i \operatorname{sen}\varphi \Rightarrow$$
$$\Rightarrow |z| = \sqrt{\cos^2\varphi + \operatorname{sen}^2\varphi} = 1$$

ii ) $e^z = 1 \Rightarrow z = 2\,n\,\pi\,i \quad \text{con} \quad n \in \mathbb{Z}$

Sea $z = x + yi$

Entonces

$$e^z = e^{x+yi} = e^x\, e^{yi} = e^x\,(\cos y + i \operatorname{sen} y) =$$
$$= e^x \cos y + e^x\, i \operatorname{sen} y = 1 + 0\,i$$

Por igualdad de complejos es

$$e^x \cos y = 1 \ \wedge \ e^x \operatorname{sen} y = 0$$

Como $e^x \neq 0$ resulta $\operatorname{sen} y = 0$ y en consecuencia $y = k\,\pi$ con $k \in \mathbb{Z}$

Ahora bien

$$y = k\,\pi \Rightarrow \cos y = \cos k\,\pi = (-1)^k$$

Luego

$$e^x\,(-1)^k = 1 = (-1)^{2k}$$

Es decir, $e^x = (-1)^k$, y como $e^x > 0$, se tiene $k = 2\,n$.

Así, $e^x = 1 \Rightarrow x = 0$

Resulta

$$z = x + yi = 0 + 2\,n\,\pi\,i = 2\,n\,\pi\,i$$

## 11.12. LOGARITMACION EN C

Sea $z \neq 0$. Por definición $\ln z = w$ si y sólo si $e^w = z$.

Para determinar los complejos $w$ que satisfacen $w = \ln z$, proponemos la forma exponencial para el complejo $z$ y la forma binómica para $w$, es decir

$$z = \rho\, e^{i\varphi} \quad \text{y} \quad w = u + iv$$

Hay que determinar $u$ y $v$ tales que

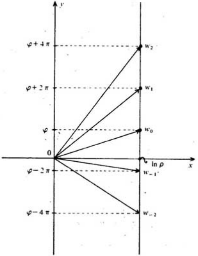
$$e^{u+iv} = \rho\, e^{i\varphi}$$
$$\Downarrow$$
$$e^{u} \,.\, e^{iv} = \rho\, e^{i\varphi}$$
$$\Downarrow$$
$$e^{u} = \rho \;\wedge\; v = \varphi + 2\,k\,\pi$$
$$\Downarrow$$
$$u = \ln \rho \;\wedge\; v = \varphi + 2\,k\,\pi$$

Resulta

$$\ln z = \ln \rho + i\,(\varphi + 2\,k\,\pi) \quad \text{con} \quad k \in \mathbf{Z}$$

fórmula que permite obtener los infinitos logaritmos de un complejo no nulo.

Como la parte real del $\ln z$ es independiente de $k$, todos los logaritmos corresponden a puntos de la paralela al eje de ordenadas que pasa por $(\ln \rho, 0)$



Valor principal de $\ln z$ es el que se obtiene para $k = 0$, o sea

$$\text{V.p. } \ln z = \ln \rho + i\,\varphi$$

***Ejemplo 11-13.***

Hallar $\ln z$ en los siguientes casos

i ) $z = -2$

$$z = -2 + 0\,i \Rightarrow \rho = 2 \;\wedge\; \varphi = \pi$$

Luego

$$\ln z = \ln(-2) = \ln 2 + i\,(\pi + 2\,k\,\pi) = \\ = \ln 2 + (1 + 2\,k)\,\pi\,i$$

ii ) $z = -\dfrac{e}{\sqrt{2}} - \dfrac{e}{\sqrt{2}}\,i$

$$\rho = \sqrt{\frac{e^2}{2} + \frac{e^2}{2}} = e \quad \wedge \quad \varphi = 225^{\circ} = 5\,\frac{\pi}{4}$$

Entonces

$$\ln z = \ln e + i\left(5\,\frac{\pi}{4} + 2\,k\,\pi\right) = \\ = 1 + i\left(5\,\frac{\pi}{4} + 2\,k\,\pi\right)$$

Los valores principales son, respectivamente, $\ln 2 + i\,\pi$ y $1 + 5\,\dfrac{\pi}{4}\,i$

## 11.13. EXPONENCIAL COMPLEJA GENERAL

Sean $z_1$ y $z_2$ tales que $z_1 \neq 0$. Estamos interesados en la determinación de la exponencial compleja

$$w = z_1^{z_2}$$

Aplicando logaritmos en base natural

$$\ln w = z_2 \ln z_1$$

Por definición de logaritmo

$$w = e^{z_2 \ln z_1}$$

***Ejemplo 11-14.***

Hallar el valor principal de la exponencial

$$z = \left(\frac{1-i}{1+i}\right)^{i}$$

Calculamos

$$\frac{1-i}{1+i}=\frac{(1-i)^2}{(1+i)(1-i)}=\frac{1-2i-1}{2}=-i$$

Entonces

$$z=(-i)^i \Rightarrow \ln z = i \ln(-i) \qquad (1)$$

Al complejo $-i$ le corresponden

$$\rho=\sqrt{0^2+(-1)^2}=1 \quad \wedge \quad \varphi=3\,\frac{\pi}{2}$$

Entonces

$$\ln(-i)=\ln 1+i\left(3\,\frac{\pi}{2}+2k\pi\right)=$$
$$=i\left(3\,\frac{\pi}{2}+2k\pi\right)$$

Sustituyendo en (1) tenemos

$$\ln z=-3\,\frac{\pi}{2}-2k\pi$$

Por definición de logaritmo resulta

$$z=e^{-3\frac{\pi}{2}-2k\pi}$$

Siendo el valor principal

$$\text{V.p. } z=e^{-3\frac{\pi}{2}}$$

## 11.14. RAICES PRIMITIVAS DE LA UNIDAD

### 11.14.1. Concepto

En el ejemplo 11-11-ii ) hemos determinado las raíces de orden 3 de la unidad, es decir, las tres raíces cúbicas de 1. Tales raíces son

$$w_0=1 \qquad w_1=-\frac{1}{2}+i\,\frac{\sqrt{3}}{2} \qquad w_2=-\frac{1}{2}-i\,\frac{\sqrt{3}}{2}$$

Las dos últimas no son raíces de la unidad de un orden menor que 3, pero la primera sí lo es, puesto que

$$\sqrt[1]{1}=1 \quad \text{ y } \quad \sqrt[2]{1}=\pm 1$$

Por este motivo se dice que $w_1$ y $w_2$ son raíces primitivas de orden 3 de la unidad; en cambio, $w_0=1$ no es raíz primitiva de orden 3 ni de orden 2, sino de orden 1.

Sea $G_n$ el conjunto de las $n$ raíces $n$-simas de la unidad. Un elemento genérico de $G_n$ es

$$w_k = \cos \frac{2k\pi}{n} + i \operatorname{sen} \frac{2k\pi}{n} = e^{i\frac{2k\pi}{n}}$$

donde $k = 0, 1, 2, \ldots, n-1$. Por definición de raíz $n$-sima, los complejos $w_k$ satisfacen la condición $w_k^n = 1$, y son tales que $(G_n, .)$ es un grupo multiplicativo abeliano. Esta situación ha sido tratada en el ejemplo 8-12, en el caso particular en que $n = 3$.

**Definición**

El elemento $w_k \in G_n$ es una raíz primitiva de orden $n$ de la unidad si y sólo si no es raíz de 1 de un orden menor que $n$.

El conjunto de las raíces cuartas de la unidad es $G_4 = \{1, i, -1, -i\}$. De acuerdo con la definición y con el conocimiento de $G_1$, $G_2$ y $G_3$, podemos decir que $i$ y $-i$ son raíces primitivas de orden 4 de la unidad. Los resultados $1, i, -1$ y $-i$ se obtienen de la fórmula general al tomar $k$ los valores 0, 1, 2 y 3, respectivamente. Observamos aquí que si $k$ es coprimo con $n$, entonces la raíz $w_k$ es primitiva. Tal es el caso de $w_1$ y $w_3$, para $n = 4$. La demostración de esta propiedad es el objeto de lo que sigue.

**11.14.2. Propiedad.** El complejo $w_k \in G_n$ es raíz $m$-sima de la unidad si y sólo si $n \mid km$.

Demostración)

Sea $w_k = \cos \frac{2k\pi}{n} + i \operatorname{sen} \frac{2k\pi}{n} = e^{i\frac{2k\pi}{n}} \in G_n$. Entonces

$$w_k = \sqrt[m]{1} \Leftrightarrow w_k^m = 1 \Leftrightarrow \cos \frac{2km\pi}{n} + i \operatorname{sen} \frac{2km\pi}{n} = 1 \Leftrightarrow$$

$$\Leftrightarrow \cos \frac{2km\pi}{n} = 1 \wedge \operatorname{sen} \frac{2km\pi}{n} = 0 \Leftrightarrow$$

$$\Leftrightarrow \frac{2km\pi}{n} = 2\pi q \wedge q \in \mathbb{Z} \Leftrightarrow$$

$$\Leftrightarrow \frac{km}{n} = q \Leftrightarrow km = nq \Leftrightarrow n \mid km$$

**11.14.3. Propiedad.** Sea $0 \leqslant k < n$. Entonces $w_k \in G_n$ es una raíz primitiva de orden $n$ de la unidad si y sólo si $n$ y $k$ son coprimos.

1) $n$ y $k$ son coprimos $\Rightarrow$ $w_k$ es raíz $n$-sima primitiva de 1.

Sea $w_k$ una raíz $m$-sima de la unidad. Entonces, por 11.14.2., se tiene que $n \mid km$ y como $n$ y $k$ son coprimos, resulta $n \mid m$, de acuerdo con lo demostrado en el ejemplo 9-8-ii). Ahora bien, siendo $n$ y $m$ números naturales y $n \mid m$, es $n \leqslant m$, y en consecuencia $w_k$ no es raíz de la unidad de un orden menor que $n$, o lo que es lo mismo, $w_k$ es raíz primitiva de orden $n$ de 1.

II) $w_k$ es raíz $n$-sima primitiva de 1 $\Rightarrow$ m.c.d. $(n, k) = 1$

Supongamos que $n$ y $k$ no son coprimos, y sea $d$ su m.c.d. positivo. Por definición de m.c.d. se tiene

$$d \mid n \wedge d \mid k \Rightarrow n = dn' \wedge k = dk' \quad \text{donde} \quad \text{m.c.d.}(n', k') = 1$$

Sustituyendo estos valores en la expresión de $w_k$ resulta

$$w_k = \cos \frac{2dk'\pi}{dn'} + i \operatorname{sen} \frac{2dk'\pi}{dn'} =$$

$$= \cos \frac{2k'\pi}{n'} + i \operatorname{sen} \frac{2k'\pi}{n'}$$

Como $n'$ y $k'$ son coprimos se deduce que $w_k$ es raíz de la unidad de orden $n' < n$, lo que contradice la hipótesis. Luego debe ser mcd $(n, k) = 1$

*Ejemplo 11-15.*

Determinar las raíces primitivas de orden 6 de la unidad.

Las seis raíces sextas de 1 están dadas por

$$w_k = \cos \frac{2k\pi}{6} + i \operatorname{sen} \frac{2k\pi}{n}$$

con $k = 0, 1, \ldots, 5$

De acuerdo con 11.14.3. I) elegimos $k$ de modo que m.c.d. $(n, 6) = 1$ y se obtiene $k = 1$ o $k = 5$. Las raíces primitivas pedidas son, entonces

$$w_1 = \cos \frac{2\pi}{6} + i \operatorname{sen} \frac{2\pi}{6} =$$

$$= \cos \frac{\pi}{3} + i \operatorname{sen} \frac{\pi}{3} = \cos 60^\circ + i \operatorname{sen} 60^\circ =$$

$$= \frac{1}{2} + i \frac{\sqrt{3}}{2}$$

$$w_5 = \cos \frac{10\pi}{6} + i \operatorname{sen} \frac{10\pi}{6} =$$

$$= \cos \frac{5\pi}{3} + i \operatorname{sen} \frac{5\pi}{3} = \cos 300^\circ + i \operatorname{sen} 300^\circ =$$

$$= \cos 60^\circ - i \operatorname{sen} 60^\circ = \frac{1}{2} - i \frac{\sqrt{3}}{2}$$

## TRABAJO PRACTICO XI

*11-16.* Dados los números complejos

$$z_1 = \sqrt{3} + i \quad z_2 = -\sqrt{3} + 3i \quad z_3 = 2 - 2\sqrt{3i}$$

efectuar

$$2z_1 - (z_2^2 - z_3) - \frac{z_2}{z_1}$$

*11-17.* Determinar los complejos $z$ en cada uno de los siguientes casos

a) $(1+i) + z = -i$ c) $z = (-i)(1+i)$

b) $z = i(1+i)$ d) $iz = (1+i)(1-i)$

*11-18.* Obtener $z$ en los siguientes casos

a) $z = (1 + \sqrt{3}i)(\sqrt{3} + i)$

b) $z = (\sqrt{2} + \sqrt{3}i)^2 - \sqrt{6}i$

c) $z = (\sqrt{2} + \sqrt{3}i)(\sqrt{3} - \sqrt{2}i)$

d) $z = \left(-\frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right)^3$

*11-19.* Resolver las siguientes ecuaciones en $z$

a) $iz = 1$ c) $(2-i)z = i$

b) $(1+i)z = 1$ d) $\frac{1}{z} = i$

*11-20.* Expresar $z$ en la forma binómica

a) $z = \dfrac{\sqrt{2} + \sqrt{3}i}{\sqrt{2} - \sqrt{3}i}$ c) $z = 1 + \cfrac{i}{1 + \cfrac{i}{1 + \cfrac{i}{1+i}}}$

b) $z = \dfrac{(3-i)(2+i)}{i}$

*11-21.* Hallar las soluciones de las siguientes ecuaciones en **C**

a) $z^2 = 2i$ b) $z^2 = -3 - 4i$ c) $z^2 = -2\sqrt{3} + 2i$

*11-22.* Obtener la forma polar de los siguientes números complejos

a) $z_1 = \sqrt{3} + i$ c) $z_3 = -1 - i$

b) $z_2 = -2 - 2\sqrt{3}i$ d) $z_4 = -3i$

*11-23.* Efectuar en forma polar las operaciones que se indican con relación a los complejos del ejercicio anterior

a) $z_1^6$  c) $\dfrac{z_3}{z_4}$

b) $z_2 z_3$  d) $z_3^{10}$

*11-24.* Calcular $z^2$ siendo

$$z = -|-1+i| + \sqrt{2}\, i$$

*11-25.* Probar que si $f(x) = ax^2 + bx + c$ donde $a$, $b$ y $c$ son números reales y $z \in \mathbf{C}$ es tal que $f(z) = 0$, entonces $f(\bar{z}) = 0$.

*11-26.* Dado $z = 1 + \operatorname{sen} a + i \cos a$, determinar $|z^2 - \bar{z}|$

*11-27.* Determinar los números reales $a$ y $b$ sabiendo que

$$(-1+i)\,a + (1+2i)\,b = 1$$

*11-28.* Resolver la ecuación en **C**

$$(z-1-i)(z-1+i)(z+1+i)(z+1-i) = 5$$

*11-29.* Resolver la ecuación en **C**

$$x^2 + (-2-2i)\,x = 3-6i$$

*11-30.* Resolver el siguiente sistema de ecuaciones en **C**

$$\begin{cases} (1+i)\,x - iy = 2+i \\ (2+i)\,x + (2-i)\,y = 2i \end{cases}$$

*11-31.* Demostrar

a) El conjugado del opuesto de todo complejo es igual al opuesto de su conjugado.

b) El conjugado de la diferencia de dos complejos es igual a la diferencia de los conjugados.

c) El módulo de la diferencia de dos complejos es mayor o igual que la diferencia de los módulos.

d) El conjugado del cociente de dos complejos es igual al cociente de sus conjugados.

e) El módulo del cociente de dos complejos es igual al cociente de sus módulos

*11-32.* Sean los complejos no nulos $z$ y $z'$. Demostrar

$$|z|^{-1}\,|z-z'|\,|z'|^{-1} = |z^{-1} - z'^{-1}|$$

*11-33.* Demostrar

$$|z+z'|^2 + |z-z'|^2 = 2\,|z|^2 + 2\,|z'|^2$$

*11-34.* Demostrar por inducción completa

$$(\cos x + i \operatorname{sen} x)^n = \cos nx + i \operatorname{sen} nx$$

*11-35.* Utilizando la fórmula de De Moivre demostrar las siguientes fórmulas

i ) $\operatorname{sen} 2x = 2 \operatorname{sen} x \cos x$

$\cos 2x = \cos^2 x - \operatorname{sen}^2 x$

ii ) $\operatorname{sen} 3x = 3\cos^2 x \operatorname{sen} x - \operatorname{sen}^3 x$

$\cos 3x = \cos^3 x - 3\cos x \operatorname{sen}^2 x$

*11-36.* Sabiendo que los complejos 1, $w$ y $w^2$ satisfacen la relación $x^3 = 1$, verificar

i ) $(1 + w^2)^4 = w$

ii ) $(1 - w + w^2)(1 + w - w^2) = 4$

*11-37.* Determinar algebraicamente las raíces cuadradas de los siguientes complejos:

i ) $z = -15 - 8i$

ii ) $z = 5 - 12i$

iii) $z = 8 + 4\sqrt{5}\,i$

*11-38.* Resolver las siguientes ecuaciones en **C**

i ) $x^2 - (2 + i)x + 3 + i = 0$

ii ) $x^2 + (-3 + 2i)x - i = 0$

*11-39.* Determinar y representar las raíces que se indican

i ) $\sqrt[4]{1 - i}$  ii ) $\sqrt[3]{-i}$  iii) $\sqrt[3]{8}$  iv) $\sqrt[3]{\sqrt{3} + i}$

*11-40.* Determinar los logaritmos naturales de los siguientes complejos

i ) $z = \sqrt{3} - \sqrt{3}\,i$

ii ) $z = -ei$

iii) $z = 4$

*11-41.* Determinar los valores principales de las exponenciales siguientes

i ) $w = (\sqrt{2} - i)^{1-i}$

ii ) $w = (3i)^{2i}$

iii) $w = (1 - i\sqrt{3})^{1/i}$

*11-42.* Obtener el valor principal de $z$ en los siguientes casos

i ) $(1 - i)^z = 1$

ii ) $\left(\dfrac{1 + i\sqrt{3}}{2}\right)^z = i$

*11-43.* Resolver las siguientes ecuaciones

i ) $x^{2i} - 2x^i + 2 = 0$

ii ) $x^{2\sqrt{3}} - x^{\sqrt{3}} + 1 = 0$

*11-44.* Determinar los conjuntos de puntos del plano que satisfacen a las siguientes relaciones

i ) $Re(z) = -2$

ii ) $-2 \leq Im(z) < 3$

iii) $|z+1| > 2$

iv) $-0{,}5 < Re(z) < 0{,}5 \ \wedge \ |z| = 2$

v ) $\frac{\pi}{4} \leq \operatorname{Arg} z \leq 3\,\frac{\pi}{4} \ \wedge \ |z| < 2$

vi) $|z - 1 + i| = 2$

*11-45.* Determinar analíticamente y gráficamente los subconjuntos de **C** que verifican

i ) $|z+1| + |z-1| = 3$

ii ) $|z+c|\,|z-c| = c^2$

*11-46.* Calcular

$$1 + 2\cos x + 2\cos 2x + \ldots + 2\cos nx$$

*11-47.* Verificar la identidad

$$\left|\frac{z+w}{2} - zw\right| + \left|\frac{z+w}{2} + zw\right| = |z| + |w|$$

*11-48.* Dado $z = -|-1+2i| + \sqrt{2\,\overline{i}}$, hallar $\ln \overline{z}$.

*11-49.* Demostrar

$$e^z = e^w \Leftrightarrow z - w = 2n\pi i \ \wedge \ n \in \mathbf{Z}$$

*11-50.* Se definen

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}, \quad \operatorname{sen} z = \frac{e^{iz} - e^{-iz}}{2i}$$

Demostrar

i ) $\cos z = \cos x \, ch\, y - i \operatorname{sen} x \, sh\, y$

ii ) $\operatorname{sen} z = \operatorname{sen} x \, ch\, y + i \cos x \, sh\, y$

*11-51.* Determinar los conjuntos de puntos del plano que verifican

i ) $z - \overline{z} = i$

ii ) $|z|^2 = z + \overline{z}$

iii) $\overline{z} - z^{-1} = 0$

iv) $z^{-1} + z = 0$

v ) $z + z^{-1} \in \mathbf{R}$

vi) $z = \overline{z}^2$

vii) $|z+i| = |z+2i|$

*11-52.* Obtener los siguientes complejos ·

$$\text{a) } z = \sum_{k=0}^{100} i^k \qquad \text{b) } z = \prod_{k=1}^{100} i^k$$

*11-53.* Los complejos no nulos $z_1$ y $z_2$ son tales que

$$|z_1 + z_2| = |z_1| + |z_2|$$

Demostrar que $z_1 = \alpha z_2$ para algún $\alpha \in \mathbf{R}^+$

*11-54.* Calcular $z^4$ siendo

i ) $z = (-\sqrt{3+i})^{-1}$

ii ) $z = \dfrac{a}{\operatorname{sen} \alpha - i \operatorname{sen} \alpha}$ con $a \in \mathbf{R} \wedge 0 \leqslant \alpha < 2\pi$

iii) $z = \dfrac{1+i}{\sqrt{3-i}}$

*11-55.* Demostrar

i ) $Re\,(z\bar{w} + \bar{z}w) = z\bar{w} + \bar{z}w$

ii ) $Im\,(z\bar{w} - \bar{z}w) = z\bar{w} - \bar{z}w$

*11-56.* Demostrar que si $w$ es raíz cúbica primitiva de 1, entonces

$$(1 - w)(1 - w^2) = 3$$

*11-57.* Sea $w$ una raíz $n$-sima primitiva de 1 y $n > 1$. Demostrar

$$\sum_{k=0}^{n-1} w^k = 0$$

*11-58.* Sabiendo que $n = 3k$, demostrar que

$$\left(-\frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right)^n + \left(-\frac{1}{2} - i\,\frac{\sqrt{3}}{2}\right)^n = 2$$

Capítulo 12

# POLINOMIOS

## 12.1. INTRODUCCION

A partir de la definición de polinomio formal de un anillo con identidad, se llega al concepto de anillo de polinomios formales de un anillo con una indeterminada, y al caso particular de dominio de integridad de polinomios de un cuerpo. En esta estructura se estudian la divisibilidad, los ideales y la factorización. El capítulo se completa con el tratamiento de los polinomios reales y complejos.

## 12.2. ANILLO DE POLINOMIOS FORMALES DE UN ANILLO

### 12.2.1. Concepto

Sea (A , + , .) un anillo con identidad.

***Definición***

Polinomio formal del anillo A es toda función $P : N_0 \rightarrow A$ que verifica $P(n) = 0$, salvo para un número finito de elementos de $N_0$.

El dominio de la función es $N_0 = \{0 , 1 , 2 , \ldots\}$, y la imagen de todo $i \in N_0$ se escribe $P(i) = a_i$. La definición dada caracteriza a todo polinomio formal como una sucesión de elementos de A cuyos términos son nulos a partir de cierto índice. Es usual identificar a un polinomio formal en términos del conjunto ordenado de las imágenes, lo que conduce a la siguiente notación

$$P = (a_0, a_1, \ldots, a_n, 0, 0, \ldots)$$

El hecho de que $P(n) = a_n$ sea distinto de cero no significa que deba ser $P(i) = a_i$ distinto de cero para $i < n$.

En particular, la función nula, definida por $P(i) = 0$ cualquiera que sea $i \in N_0$ se llama polinomio nulo, y lo indicaremos así:

$$\mathbf{0} = (0 , 0 , \ldots)$$

**Definición**

Grado de un polinomio no nulo es el mayor entero $n$ que satisface $P(n) \neq 0$.

El grado de todo polinomio no nulo se identifica con el índice del último término distinto de cero de la sucesión que lo define. Convenimos, además, que el polinomio nulo carece de grado. Algunos autores le atribuyen grado $-1$. En otros casos se le asigna grado infinito.

*Ejemplo 12-1.*

Determinamos los grados de los siguientes polinomios de los anillos que se indican

i ) El polinomio $P : N_0 \to Z_5$ definido por

$$P(0) = \overline{1},\ P(i) = P(i-1) + \overline{1} \text{ si } i = 1, 2, 3,\ P(i) = \overline{0} \text{ si } i > 3$$

es $P = (\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{0}, \overline{0}, \dots)$

siendo grado de $P = g\,P = 3$

ii ) El polinomio $Q : N_0 \to Z$ tal que

$$Q(n) = \begin{cases} -2 & \text{si } n = 4 \\ 0 & \text{si } n \neq 4 \end{cases}$$

es la sucesión

$$Q = (0, 0, 0, 0, -2, 0, 0, \dots)$$

y tiene grado 4. Todo polinomio con a lo sumo un término no nulo se llama monomio.

iii) Si el anillo es $(R^{2\times 2}, +, .)$ y definimos

$$R : N_0 \to R^{2\times 2} \text{ mediante}$$

$$R(0) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \qquad R(1) = \begin{bmatrix} 1 & 2 \\ 1 & \sqrt{2} \end{bmatrix} = A$$

y $R(n) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = N$ para todo $n > 1$, entonces

$$R = (I, A, N, N, \dots)$$

tiene grado 1.

## 12.2.2. Anillo de polinomios formales del anillo A

Sea $P$ el conjunto de todos los polinomios formales del anillo A. Es decir

$$P = \left\{ P \,/\, P : N_0 \to A \right\}$$

En $P$ definimos la adición y multiplicación mediante

I. $P + Q : N_0 \to A$ es tal que

$$(P + Q)(n) = P(n) + Q(n)$$

II. $P . Q : N_0 \to A$ es tal que

$$(P . Q)(n) = \sum_{i=0}^{n} P(i)\, Q(n - i)$$

***Ejemplo 12-2.***

Sean $P = (a_0 , a_1 , a_2 , 0 , 0 , 0 , \ldots)$ y $Q = (b_0 , b_1 , b_2 , b_3 , 0 , 0 , \ldots)$, donde $gP = 2$ y $gQ = 3$. De acuerdo con las definiciones dadas se tiene

i ) $S = P + Q$
siendo $c_i = S(i) = (P + Q)(i) = P(i) + Q(i) = a_i + b_i$ para todo $i \in N_0$.
Entonces

$$S = P + Q = (a_0 + b_0, a_1 + b_1, a_2 + b_2, b_3, 0, 0, \ldots)$$

Siendo $g(P + Q) = 3$

ii ) $R = P . Q$ se obtiene de la siguiente manera:

$$c_0 = R(0) = (PQ)(0) = \sum_{i=0}^{0} P(i)\, Q(0 - i) = P(0)\, Q(0) = a_0\, b_0$$

$$c_1 = R(1) = (PQ)(1) = \sum_{i=0}^{1} P(i)\, Q(1 - i) =$$
$$= P(0)\, Q(1) + P(1)\, Q(0) = a_0\, b_1 + a_1\, b_0$$

$$c_2 = R(2) = (PQ)(2) = \sum_{i=0}^{2} P(i)\, Q(2 - i) =$$
$$= P(0)\, Q(2) + P(1)\, Q(1) + P(2)\, Q(0) = a_0\, b_2 + a_1\, b_1 + a_2\, b_0$$

El término genérico del producto es

$$c_k = \sum_{i=0}^{k} P(i)\, Q(k - i) = \sum_{i=0}^{k} a_i\, b_{k-i}$$

Por ejemplo

$$c_5 = a_0\, b_5 + a_1\, b_4 + a_2\, b_3 + a_3\, b_2 + a_4\, b_1 + a_5\, b_0$$

En nuestro caso se reduce a

$$c_5 = a_2\, b_3$$

Pero $c_6 = c_7 = \ldots = 0$

El grado del producto es 5 si $a_2\, b_3 \neq 0$, es decir, si el anillo no tiene divisores de cero.

*Ejemplo 12-3.*

Efectuar la suma y el producto de los polinomios de $\mathbf{Z}_6$

$$P = (\bar{2}, \bar{3}, \bar{0}, \bar{0}, \bar{0}, \ldots)$$
$$\text{y} \quad Q = (\bar{0}, \bar{1}, \bar{2}, \bar{0}, \bar{0}, \ldots)$$

i ) $P + Q = (\bar{2}, \bar{4}, \bar{2}, \bar{0}, \bar{0}, \ldots)$ y $g(P+Q) = 2$

ii ) $PQ = (\bar{0}, \bar{2}, \bar{1}, \bar{0}, \bar{0}, \ldots)$ y $g(PQ) = 2$

Se verifica que $(P, +)$ tiene estructura de grupo abeliano siendo neutro para la adición el polinomio nulo, y el inverso aditivo u opuesto de cada polinomio P es el polinomio $-P$ definido por $(-P)(n) = -P(n)$.

El producto es asociativo en $P$, con identidad

$$1 : N_0 \to A \text{ tal que}$$

$$1(n) = \begin{cases} 1 & \text{si } n = 0 \\ 0 & \text{si } n \neq 0 \end{cases}$$

Es decir

$$1 = (1, 0, 0, \ldots)$$

ya que $P \in P \Rightarrow P1 = 1P = P$

Además, el producto es distributivo respecto de la suma a izquierda y a derecha

$$(P+Q)R = PR + QR$$
$$R(P+Q) = RP + RQ$$

En efecto, utilizando las definiciones de multiplicación, de adición, propiedades de la sumatoria, y del anillo A se tiene

$$[(P+Q)R](n) = \sum_{i=0}^{n} (P+Q)(i)\, R(n-i) =$$

$$= \sum_{i=0}^{n} [P(i) + Q(i)]\, R(n-i) = \sum_{i=0}^{n} [P(i)\, R(n-i) + Q(i)\, R(n-i)] =$$

$$= \sum_{i=0}^{n} P(i)\, R(n-i) + \sum_{i=0}^{n} Q(i)\, R(n-i) = (PR)(n) + (QR)(n) =$$

$$= (PR + QR)(n)$$

Las consideraciones anteriores nos permiten afirmar que la terna $(P, +, .)$ es un anillo con identidad, llamado anillo de los polinomios formales del anillo A.

El polinomio $X = (0, 1, 0, 0, \ldots)$ recibe el nombre de indeterminada. Nos proponemos expresar a todo polinomio formal del anillo A, en función de la indeterminada X y de los elementos de A.

Definimos primero la función

$$f : A \to P \quad \text{mediante} \quad f(a) = (a, 0, 0, \ldots)$$

Esta definición caracteriza un morfismo inyectivo de A en $P$, es decir, un monomorfismo. En consecuencia, $f$ es un isomorfismo de A en $f(A) \subset P$, lo cual permite identificar a cada elemento $a \in A$ con su imagen $f(a) \in P$. Desde este punto de vista, podemos decir que A es un subanillo de $P$.

Definimos $X^0 = (1, 0, 0, \ldots)$ y $X^{h+1} = X^h X$

Resulta

$$X^2 = XX = (0, 0, 1, 0, 0, \ldots)$$

Esto significa que $\forall\, m \in N_0$ se tiene

$$X^m : A \to P \quad \text{tal que} \quad X^m(n) = \begin{cases} 1 & \text{si } n = m \\ 0 & \text{si } n \neq m \end{cases}$$

Entonces, teniendo en cuenta las definiciones de adición y de multiplicación, las sucesivas potencias de la indeterminada X y el isomorfismo indicado, todo polinomio $P \in P$ puede expresarse

$$\begin{aligned} P &= (a_0, a_1, \ldots, a_n, 0, 0, \ldots) = \\ &= (a_0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots) + \ldots + (0, \ldots, a_n, 0, 0, \ldots) = \\ &= (a_0, 0, 0, \ldots)(1, 0, 0, \ldots) + (a_1, 0, 0, \ldots)(0, 1, 0, 0, \ldots) + \\ &\quad + (a_2, 0, 0, \ldots)(0, 0, 1, 0, 0, \ldots) + \ldots + (a_n, 0, 0, \ldots)(0, \ldots, 0, 1, 0, 0, \ldots) = \\ &= a_0 X^0 + a_1 X^1 + a_2 X^2 + \ldots + a_n X^n = \sum_{i=0}^{n} a_i X^i \end{aligned}$$

En lo sucesivo, en lugar de $X^0 = (1, 0, 0, \ldots) = 1$ escribiremos 1, omitiremos los términos del tipo $0X^n$ y $1X^n$ será sustituido por $X^n$

Se tiene

$$\sum_{i=0}^{n} a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

Siendo $a_n$ el coeficiente principal y $a_0$ el término independiente.

El anillo de polinomios de A en la indeterminada X suele indicarse mediante el símbolo $P = A[X]$. Los elementos de $A[X]$ se llaman polinomios en X con coeficientes en el anillo A. En particular, los elementos de $A \subset A[X]$ se llaman constantes. Si $gP = n$, entonces $a_n$ se llama coeficiente principal. Un polinomio con el coeficiente principal igual a 1 se dice que es mónico.

De acuerdo con las definiciones de las operaciones en $A[X]$, se verifican las siguientes proposiciones:

i ) El grado de todo polinomio no nulo es igual al grado de su opuesto.

$$g(-\mathrm{P}) = g\mathrm{P}$$

ii ) El grado de la suma de dos polinomios no nulos es menor o igual que el mayor de los grados.

$$g(\mathrm{P}+\mathrm{Q}) \leqslant \text{máx}\left\{g\mathrm{P}\,,g\mathrm{Q}\right\}$$

iii) El grado del producto de dos polinomios, si es no nulo, es menor o igual que la suma de los grados.

$$g(\mathrm{PQ}) \leqslant g\mathrm{P} + g\mathrm{Q}$$

Ahora bien, si A es un dominio de integridad, entonces A[X] también lo es, y se verifica que el grado del producto de dos polinomios no nulos es igual a la suma de los grados, o sea

$$g(\mathrm{PQ}) = g\mathrm{P} + g\mathrm{Q}$$

*Ejemplo 12-4.*

En $Z_5$ [X] se consideran los polinomios

$$\mathrm{A} = \overline{3}\,\mathrm{X}^2 + \overline{1}\,\mathrm{X} + \overline{2} \qquad \mathrm{B} = \overline{2}\,\mathrm{X} + \overline{1} \quad \text{y} \quad \mathrm{C} = \overline{1}\,\mathrm{X}^3 + \overline{4}\,\mathrm{X} + \overline{2}$$

Obtener el polinomio AB − C. La mecánica de las operaciones entre polinomios en la indeterminada X con coeficientes en el anillo se realiza en la forma habitual aprendida en la escuela secundaria.

$$\begin{array}{rrrrr}
\text{A:} & & \overline{3}\,\mathrm{X}^2 & +\overline{1}\,\mathrm{X} & +\overline{2} \\
\text{B:} & & & \overline{2}\,\mathrm{X} & +\overline{1} \\
\hline
 & \overline{1}\,\mathrm{X}^3 & +\overline{2}\,\mathrm{X}^2 & +\overline{4}\,\mathrm{X} & \\
 & & \overline{3}\,\mathrm{X}^2 & +\overline{1}\,\mathrm{X} & +\overline{2} \\
\hline
\text{AB:} & \overline{1}\,\mathrm{X}^3 & +\overline{0}\,\mathrm{X}^2 & +\overline{0}\,\mathrm{X} & +\overline{2}
\end{array}$$

El inverso aditivo de C es $-\mathrm{C} = \overline{4}\mathrm{X}^3 + \overline{1}\mathrm{X} + \overline{3}$

Y resulta $\mathrm{AB} - \mathrm{C} = \overline{0}\mathrm{X}^3 + \overline{0}\mathrm{X}^2 + \overline{1}\mathrm{X} + \overline{0}$

Es decir, AB − C = X.

## 12.3. ANILLO DE POLINOMIOS DE UN CUERPO

Como todo cuerpo K es un dominio de integridad, el anillo de polinomios de K, que denotamos con K [X], es un dominio de integridad, pero no es un cuerpo. En efecto, no todo polinomio no nulo admite inverso multiplicativo. Demostramos a continuación que únicamente los polinomios de grado cero son inversibles.

**Teorema.** Un polinomio de K [X] admite inverso multiplicativo si y sólo si es de grado cero.

Demostración)

Sea $P \in K[X]$ un polinomio con inverso multiplicativo. Entonces, existe $Q \in K[X]$ tal que

$$PQ = QP = 1$$

Por ser K [X] un dominio de integridad, se tiene

$$gP + gQ = g1 = 0$$

Y como los grados son enteros no negativos, resulta

$$gP = gQ = 0$$

Recíprocamente, si $gP = 0$ entonces $P = a_0 \neq 0$.

Y, como $a_0$ es un elemento no nulo de K, admite inverso multiplicativo $a_0^{-1}$. Es decir, existe

$$P^{-1} = a_0^{-1}$$

## 12.4. DIVISIBILIDAD EN EL DOMINIO K [X]

### 12.4.1. División de polinomios

**Teorema.** Dados dos polinomios A y B en K [X], siendo B no nulo, existen y son únicos dos polinomios Q y R, que verifican

i ) $A = BQ + R$

ii ) $R = \mathbf{0} \ \vee \ gR < gB$

Demostración)

Sea $gB = m$. Se presentan los siguientes casos:

I. $A = \mathbf{0} \ \vee \ gA < m \Rightarrow Q = \mathbf{0} \ \wedge \ R = A$ satisfacen las condiciones de la tesis.

II. $gA = n \geqslant m = gB$

Sean

$$A = \sum_{i=0}^{n} a_i X^i \quad \text{y} \quad B = \sum_{i=0}^{m} b_i X^i$$

Entonces $\qquad a_n \neq 0 \quad \text{y} \quad b_m \neq 0$

A expensas de A y de B podemos generar un polinomio de grado menor que A o bien el polinomio nulo, restando de A el producto de B por un polinomio conveniente del tipo $c_p X^p$.

En efecto, sean

$$Q_1 = \frac{a_n}{b_m} X^{n-m} \quad y \quad A_1 = A - Q_1 B$$

Resulta $A_1 = \mathbf{0} \vee gA_1 < gA$, pues el polinomio $Q_1 B$ es de grado $n$ y su coeficiente principal es $a_n$.

Si $A_1 \neq \mathbf{0}$ y $gA_1 \geqslant gB$, el procedimiento puede reiterarse obteniéndose $A_2$ tal que

$$A_2 = \mathbf{0} \vee gA_2 < gA_1$$

En general, si $A_j \neq \mathbf{0} \wedge gA_j \geqslant gB$, llamando

$$A_j = \sum_{i=0}^{t} c_i X^i \quad \text{con} \quad c_t \neq 0$$

se definen

$$Q_{j+1} = \frac{c_t}{b_m} X^{t-m}$$

y

$$A_{j+1} = A_j - Q_{j+1} B$$

Los enteros no negativos $gA, gA_1, gA_2, \ldots$ forman una sucesión decreciente y en consecuencia se llega a la existencia de $A_h$ tal que

$$A_h = \mathbf{0} \vee gA_h < m$$

Resulta

$$A_h = A_{h-1} - Q_h B = A_{h-2} - (Q_h + Q_{h-1}) B = \ldots =$$
$$= A - (Q_1 + Q_2 + \ldots + Q_h) B$$

Entonces, llamando R a $A_h$ y Q a $\sum_{j=1}^{h} Q_j$, se verifica

$$A = BQ + R \wedge (R = \mathbf{0} \vee gR < gB)$$

La demostración de las unicidades de Q y R se proponen como ejercicio.

Los polinomios Q y R, que verifican el teorema, se llaman el cociente y el resto de la división de A por B.

***Ejemplo 12-5.***

Obtener el cociente y el resto de las divisiones de los siguientes polinomios de $\mathbf{R}[X]$

i ) $A = X^4 + X^2 + 1 \qquad B = X^2 + X + 1$

La operación se realiza en la forma habitual ordenando ambos polinomios según las potencias decrecientes de X y completando el dividendo.

$$
\begin{array}{rrr|l}
X^4 & +X^2 & +1 & X^2+X+1 \\ \cline{4-4}
X^4+X^3+X^2 & & & X^2-X+1 \\ \cline{1-2}
-X^3 & & +1 & \\
-X^3-X^2-X & & & \\ \cline{1-3}
& X^2+X+1 & & \\
& X^2+X+1 & & \\ \cline{2-3}
& 0 & &
\end{array}
$$

ii) $A = -\frac{1}{2}X^3 \qquad B = \frac{1}{4}X + 2$

$$
\begin{array}{lll|l}
-\frac{1}{2}X^3 & & & \frac{1}{4}X+2 \\ \cline{4-4}
-\frac{1}{2}X^3-4X^2 & & & -2X^2+16X-128 \\ \cline{1-1}
4X^2 & & & \\
4X^2+32X & & & \\ \cline{1-2}
& -32X & & \\
& -32X-256 & & \\ \cline{2-2}
& 256 & &
\end{array}
$$

### 12.4.2. Caso particular

Si el dividendo A es de grado $n$ y el divisor es de grado 1, es decir $B = b_1 X + b_0$, entonces, de acuerdo con el algoritmo de la división, el cociente Q es de grado $n-1$ y el resto es el polinomio nulo o bien de grado cero, es decir, puede identificarse con una constante en K, y se tiene

$$A = B \cdot Q + r$$

En el caso en que el divisor sea de primer grado y mónico es posible obtener el cociente y el resto, mediante el procedimiento conocido como Regla de Ruffini.

Sean $A = a_n X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_1 X + a_0$

$B = X + b_0 = X - a$, siendo $a = -b_0$.

Entonces, los coeficientes del cociente y el resto, que se obtienen utilizando el procedimiento indicado en 12.4.1., son

$$c_{n-1} = a_n$$
$$c_{n-2} = a_{n-1} + c_{n-1}\, a$$
$$c_{n-3} = a_{n-2} + c_{n-2}\, a$$
$$\dots\dots\dots\dots\dots$$
$$c_0 \quad = a_1 + c_1\, a$$

y $r = a_0 + c_0\, a$. Estos resultados pueden lograrse con la siguiente disposición práctica

| | | | | |
|---|---|---|---|---|
| | $a_n$ | $a_{n-1}\ \ a_{n-2} \dots\ a_1$ | $a_0$ | + |
| $a$ | | $ac_{n-1}\ \ ac_{n-2} \dots ac_1$ | $ac_0$ | |
| | $c_{n-1}$ | $c_{n-2}\ \ c_{n-3} \dots\ c_0$ | $r$ | |

*Ejemplo 12-6.*

Mediante la regla de Ruffini, obtener el cociente y el resto de la división de $A = -X^3 + 2$ por $B = X - 2$

| | | | | |
|---|---|---|---|---|
| | $-1$ | $0$ | $0$ | $2$ |
| $2$ | | $-2$ | $-4$ | $-8$ |
| | $-1$ | $-2$ | $-4$ | $-6$ |

Resulta

$$Q = -X^2 - 2X - 4 \quad y \quad r = -6$$

### 12.4.3. Relación de divisor en K [X]

Por definición, el polinomio B es divisor de A si y sólo si existe C tal que $A = BC$. Se dice también que A es múltiplo de B. Si $B \neq 0$, entonces la definición anterior equivale a decir que el resto de la división de A por B es el polinomio nulo.

Se verifican las siguientes propiedades

I. Si un polinomio es divisor de otro, entonces es divisor de su producto por cualquier polinomio.

$$A|B \Rightarrow A|BC$$

II. Si un polinomio es divisor de otros dos, entonces es divisor de su suma.

$$A|B \ \wedge\ A|C \Rightarrow A|B + C$$

III. Si el dividendo y el divisor se multiplican por un mismo polinomio no nulo, entonces el cociente no varía, pero el resto queda multiplicado por dicho polinomio.

Hipótesis) $\begin{array}{l|l} A & B \\ \hline R & Q \end{array}$ $C \neq 0$ Tesis) $\begin{array}{l|l} AC & BC \\ \hline RC & Q \end{array}$

Demostración)

Por hipótesis

$$A = BQ + R \quad y \quad R = 0 \ \vee \ gR < gB$$

Multiplicando la primera igualdad por C, utilizando la distributividad, asociatividad y conmutatividad en K [X], se tiene

$$AC = BQC + RC = (BC)\,Q + (RC) \qquad (1)$$

Por otra parte

$$g\,(RC) = gR + gC < gB + gC = g\,(BC) \ \vee \ RC = 0 \qquad (2)$$

Las proposiciones (1) y (2) verifican la tesis.

***Ejemplo 12-7.***

Dados $A = 4X^3 + 2X + 1$ y $B = 2X - 4$, obtener el cociente y el resto utilizando la regla de Ruffini. Teniendo en cuenta la propiedad III, podemos aplicar la regla dividiendo A y B por 2, es decir, multiplicando a ambos por el polinomio 1/2, a fin de que el divisor sea mónico.

Entonces $\frac{1}{2}\,A = 2X^3 + X + \frac{1}{2}$ y $\frac{1}{2}\,B = X - 2$

$$\begin{array}{c|ccc|c} & 2 & 0 & 1 & \frac{1}{2} \\ 2 & & 4 & 8 & 18 \\ \hline & 2 & 4 & 9 & \frac{37}{2} \end{array}$$

Resulta

$$Q = 2X^2 + 4X + 9 \quad y \quad \frac{1}{2}\,R = \frac{37}{2} \quad \text{es decir} \quad R = 37$$

## 12.5. IDEALES DE K [X]

De acuerdo con 9.6.2., el subanillo I de K [X] es un ideal si y sólo si

$$A \in I \ \wedge \ P \in K[X] \Rightarrow AP \in I$$

Ideales triviales del anillo K [X] son el mismo K[X] y el conjunto cuyo único elemento se reduce al polinomio nulo. Este se llama ideal nulo de K [X].

**Teorema.** Todo ideal de K [X] es principal.

Demostración)

Se trata de probar que todo ideal de K [X] está generado por un único polinomio. Distinguimos dos casos

i ) Si I es el ideal nulo, entonces está generado por el polinomio nulo, y en consecuencia es principal.

ii ) Sea $I \neq \{0\}$ un ideal no nulo de K [X]. Entonces existe en I un polinomio no nulo. Como los grados son enteros no negativos, de acuerdo con el principio de buena ordenación, I contiene a un polinomio de grado mínimo. Sea éste B. Ahora bien, si $A \in I$, por el algoritmo de la división, existen en K [X] dos polinomios Q y R, únicos, tales que

$$A = BQ + R \quad y \quad R = 0 \ \vee \ gR < gB$$

O sea

$$R = A - BQ$$

Por definición de ideal

$$A \in I \ \wedge \ B \in I \Rightarrow A \in I \ \wedge \ BQ \in I \Rightarrow A - BQ \in I \Rightarrow R \in I$$

Como B es de grado mínimo en I, no puede ser $gR < gB$, y en consecuencia $R = 0$. Es decir

$$A = BQ$$

Esto significa que I está generado por el polinomio B, de grado mínimo, o, lo que es lo mismo, I es un ideal principal.

## 12.6. FACTORIZACION EN K[X]

### 12.6.1. Máximo común divisor

Sean A y B dos polinomios no simultáneamente nulos del dominio de integridad principal K [X].

***Definición***

El polinomio D es un máximo común divisor de A y B si y sólo si es divisor de ambos y, además, múltiplo de todo divisor común.

$$D \text{ es un m.c.d. de } A \text{ y } B \Leftrightarrow \begin{cases} D | A \ \wedge \ D | B \\ D' | A \ \wedge \ D' | B \Rightarrow D' | D \end{cases}$$

**Teorema.** Todo máximo común divisor de dos polinomios A y B es una combinación lineal de los mismos con coeficientes en K [X].

Demostración)

Sea I el ideal de K [X] generado por los polinomios A y B.

Es decir

$$I = \left\{PA + QB \,/\, P \in K[X] \ \wedge \ Q \in K[X]\right\}$$

Como todo ideal de K [X] es principal, I está generado por un polinomio D de grado mínimo, es decir, existen S y T en K [X] tales que

$$D = SA + TB \qquad (1)$$

Por otra parte

$$A = 1 \,.\, A + 0 \,.\, B \ \wedge \ B = 0 \,.\, A + 1 \,.\, B \Rightarrow A \in I \ \wedge \ B \in I$$

O sea, A y B son múltiplos de D, o lo que es lo mismo, D es un divisor común de A y B.

Sea ahora

$$D' | A \ \wedge \ D' | B \Rightarrow A = MD' \ \wedge \ B = ND'$$

Sustituyendo en (1)

$$D = SMD' + TND' = (SM + TN)\, D'$$

Luego

$$D' | D$$

En consecuencia, D = SA + TB es un máximo común divisor de A y B.

**Propiedad.** Si D y D' son máximos comunes divisores de A y B, entonces existe

$$a \in K \quad \text{tal que} \quad D = aD'.$$

Demostración)

Por ser D' un m.c.d. de A y B, se verifica

$$D' | A \ \wedge \ D' | B$$

Y como D también lo es, se tiene

$$D' | D$$

Por definición de divisor existe R en K [X] tal que

$$D = D'R$$

Por grado del producto

$$gD = gD' + gR$$

Y como los grados son enteros no negativos, resulta

$$gD \geqslant g\, D' \qquad (1)$$

Análogamente

$$gD' \geqslant gD \qquad (2)$$

De (1) y (2), por la antisimetría de la relación de mayor o igual, es

$$gD = gD'$$

O sea, $gR = 0$. Esto nos permite identificar al polinomio R de grado 0, con una constante no nula $a$, de K.

Luego

$$D = aD'$$

Siendo todos los m.c.d. de A y B del mismo grado, convenimos en llamar máximo común divisor de A y B al único m.c.d. mónico, y escribiremos m.c.d. (A , B).

***Ejemplo 12-8.***

Determinamos el m.c.d. de A y B en los siguientes casos

i ) $A = \bar{3}\,X^3 \quad B = \bar{4}\,X^2 \quad$ en $Z_5\,[X]$.

Resulta m.c.d. (A y B) = $X^2$.

ii ) $A = -2\,X^2 + 2\,X \quad B = \sqrt{3}\;X - \sqrt{3} \quad$ en $R\,[X]$

Se tiene m.c.d. (A y B) = $X - 1$.

## 12.6.2. Determinación del m.c.d. por divisiones sucesivas

La propiedad demostrada en 9.14.2. es válida en K [X] y nos permite afirmar que el m.c.d. de los polinomios A y B es igual al m.c.d. entre B y el resto de la división de A por B, siendo $B \neq 0$.

El esquema de las divisiones sucesivas propuesto para los enteros en 9.14.3. adopta aquí la forma análoga siguiente

| | $Q_1$ | $Q_2$ | ...... | $Q_{n-1}$ | $Q_n$ | $Q_{n+1}$ |
|---|---|---|---|---|---|---|
| A | B | $R_1$ | ............ | | $R_{n-1}$ | $R_n$ |
| $R_1$ | $R_2$ | ... | ........ | $R_n$ | 0 | |

En consecuencia

$$\text{m.c.d.}\,(A\,,B) = \text{m.c.d.}\,(B\,,R_1) = \text{m.c.d.}\,(R_1\,,R_2) = \ldots = \text{m.c.d.}\,(R_{n-1}\,,R_n) =$$
$$= \text{m.c.d.}\,(R_n\,,0) = R_n$$

siendo $R_n$ el último resto no nulo de las divisiones sucesivas.

*Ejemplo 12-9.*

Determinar el m.c.d. de $A = X^5 + X^3 - 2X^2 + X - 1$ y $B = X^4 - 2X + 1$ por divisiones sucesivas.

| | | | |
|---|---|---|---|
| | $X$ | $X$ | $X^2 + X + 1$ |
| $X^5 + X^3 - 2X^2 + X - 1$ | $X^4 - 2X + 1$ | $X^3 \quad -1$ | $X - 1$ |
| $X^5 \quad - 2X^2 + X$ | $X^4 - X$ | $X^3 - X^2$ | |
| $X^3 \quad -1$ | $-X + 1$ | $X^2 \quad -1$ | |
| | $X - 1$ | $X^2 - X$ | |
| | | $X - 1$ | |
| | | $X - 1$ | |
| | | $0$ | |

Resulta m.c.d. $(A, B) = X - 1$.

### 12.6.3. Polinomios coprimos

Sean A y B dos polinomios no simultáneamente nulos de $K[X]$.

***Definición***

Los polinomios A y B de $K[X]$ son coprimos si y sólo si todo divisor común de A y B es inversible.

Equivalentemente, podemos decir que A y B son coprimos si y sólo si todo m.c.d. de A y B es de grado cero. Como el polinomio mónico de grado cero es 1, se tiene

$$A \text{ y } B \text{ coprimos} \Leftrightarrow \text{m.c.d.}(A \text{ y } B) = 1$$

En consecuencia, de acuerdo con el teorema 12.6.1., resulta

$$A \text{ y } B \text{ coprimos} \Leftrightarrow \exists\, S \text{ y } T \text{ en } K[X] \,/\, SA + TB = 1$$

*Ejemplo 12-10.*

En $R[X]$ se consideran los polinomios

$$A = X^3 + X^2 \quad \text{y} \quad B = X - 1$$

Por el algoritmo de la división existen

$$Q = X^2 + 2X + 2 \quad \text{y} \quad R = 2$$

tales que

$$X^3 + X = (X^2 + 2X + 2)(X - 1) + 2$$

Entonces

$$(X^3+X)-(X^2+2X+2)(X-1)=2$$

O sea

$$\frac{1}{2}(X^3+X)+\left(-\frac{1}{2}X^2-X-1\right)(X-1)=1$$

Es decir, hemos expresado al polinomio 1 como combinación lineal de A y B con coeficientes $S=\frac{1}{2}$ y $T=-\frac{1}{2}X^2-X-1$, de lo que se deduce que A y B son coprimos.

### 12.6.4. Polinomio primo o irreducible

Sabemos que los únicos polinomios inversibles de K [X] son las constantes no nulas de K. Dado $A = X + 1$, ocurre que las únicas descomposiciones de A en el producto de dos polinomios P y Q son tales que P es inversible o Q es inversible. Es decir, no es posible descomponer a A en el producto de dos polinomios de grados positivos. Se dice entonces que A es primo o irreducible en **R** [X].

***Definición***

El polinomio no inversible $A \in K[X]$ es primo o irreducible si y sólo si toda descomposición $A = PQ$ es tal que alguno de los factores es inversible.

O bien

A es irreducible si y sólo si no existen P y Q tales que

$$A = PQ \quad \text{con} \quad gP > 0 \;\wedge\; gQ > 0$$

***Ejemplo 12-11.***

i ) Todos los polinomios de grado 1 son irreducibles en K [X], pues ningún polinomio del tipo $A = a_1X + a_0$ con $a_1 \neq 0$ puede descomponerse en el producto de dos polinomios de grado mayor que cero.

ii ) No todo polinomio de grado 2 es irreducible en **R** [X].
En efecto, $A = aX^2 + bX + c$ con $b^2 - 4ac < 0$ es irreducible, pero si $b^2 - 4ac \geqslant 0$, entonces A es reducible, es decir, puede expresarse como el producto de dos polinomios reales de grado 1.

**12.6.5. Propiedades.** En el dominio principal K [X] se verifican las siguientes proposiciones, cuyas demostraciones son análogas a las desarrolladas en el Capítulo 9:

**I. Si un polinomio primo es divisor de un producto, entonces es divisor de alguno de los factores.**

$$P \text{ es primo} \;\wedge\; P|AB \Rightarrow P|A \;\vee\; P|B$$

II. Si un polinomio es divisor de un producto y es coprimo con uno de los factores, entonces es divisor del otro.

$$P|AB \ \wedge \ \text{m.c.d.}(P \text{ y } A) = 1 \Rightarrow P|B$$

**12.6.6. Teorema fundamental de la descomposición factorial.** Todo polinomio no nulo en K [X] puede expresarse como el producto de una constante por polinomios mónicos irreducibles. Tal descomposición es única, excepto el orden de los factores.

Demostración)

Distinguimos dos casos:

I. Si A es una constante no nula o un polinomio irreducible en K [X], el teorema se cumple obviamente, pues

$$A = a = a \cdot 1$$

O bien

$$A = \sum_{i=0}^{n} a_i X^i = a_n \sum_{i=0}^{n} \frac{a_i}{a_n} X^i$$

II. Sea A de grado $m$, reducible en K [X]. Entonces existen en K [X] dos polinomios $P_1$ y $P_2$ de grados positivos, tales que

$$A = P_1 P_2 \qquad (1)$$

Supongamos que la descomposición es válida para todo $k < m$, es decir

$$P_1 = a_1 \prod_{i=1}^{t} P'_{1i} \quad \text{y} \quad P_2 = a_2 \prod_{j=1}^{u} P'_{2j}$$

donde $a_1$ y $a_2$ son constantes y los polinomios $P'_{1i}$ y $P'_{2j}$ son mónicos irreducibles. Multiplicando las dos últimas relaciones se tiene

$$P_1 P_2 = (a_1 a_2) \left( \prod_{i=1}^{t} P'_{1i} \right) \left( \prod_{j=1}^{u} P'_{2j} \right)$$

Teniendo en cuenta (1) resulta

$$A = a \prod_{h=1}^{r} P''_h$$

siendo $a$ una constante $h = t + u$ y los $P_h$ polinomios mónicos irreducibles. O sea, la descomposición es válida para $m$, y en consecuencia lo es para todo $n \in N$, de acuerdo con el segundo principio de inducción completa.

Para probar la unicidad de la descomposición factorial, suponemos que A admite dos descomposiciones

$$A = a P_1 P_2 \dots P_r \quad \text{y} \quad A = b Q_1 Q_2 \dots Q_s$$

Como $a$ y $b$ son el coeficiente principal de A, se tiene $a = b$. Entonces

$$P_1 P_2 \ldots P_r = Q_1 Q_2 \ldots Q_s \qquad (2)$$

Ahora bien

$$P_1 | A \quad y \quad P_1 \text{ primo} \Rightarrow P_1 | Q_i \text{ para algún } i \text{ por 12.6.5. I.}$$

Entonces, $Q_i = RP_1$, pero como $Q_i$ es irreducible debe ser R una constante, y además igual a 1, ya que ambos son polinomios mónicos. En consecuencia, $P_1 = Q_i$.

Luego de dividir (2) por esta igualdad resulta

$$P_2 P_3 \ldots P_r = \underset{j \neq i}{\pi} Q_j$$

Reiterando el proceso, de acuerdo con el segundo principio de inducción completa, los $P_k$ son iguales dos a dos a los $Q_j$, y la descomposición es única.

***Ejemplo 12-12.***

Descomposición factorial de los siguientes polinomios en **R** [X] y en **C** [X].

i ) $P = X^6 - X^5 + X^4 - X^3 = X^3 (X^3 - X^2 + X - 1) =$
$= X^3 [X^2 (X-1) + (X-1)] = X^3 (X^2 + 1)(X-1)$

Esta es la descomposición de P en cinco factores mónicos irreducibles en **R** [X]. El exponente 3 del factor irreducible X es el mayor entero que satisface $X^3 | P$. Además, $X^2 + 1$ es irreducible en **R** [X], pues $b^2 - 4ac = 0 - 4 < 0$.

En cambio, en **C** [X] la descomposición factorial es

$$P = X^3 (X + i)(X - i)(X - 1)$$

ii ) $Q = X^4 + X^2 + 1 = X^4 + 2X^2 + 1 - X^2 = (X^2 + 1)^2 - X^2 =$
$= (X^2 + X + 1)(X^2 - X + 1)$

que son irreducibles en **R** [X], pero no en **C** [X], pues

$$X^2 + X + 1 = X^2 + X + \frac{1}{4} + \frac{3}{4} =$$
$$= \left(X + \frac{1}{2}\right)^2 - \left(\frac{\sqrt{3}}{2}\, i\right)^2 = \left(X + \frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right)\left(X + \frac{1}{2} - i\,\frac{\sqrt{3}}{2}\right)$$

Análogamente

$$X^2 - X + 1 = \left(X - \frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right)\left(X - \frac{1}{2} - i\,\frac{\sqrt{3}}{2}\right)$$

## 12.7. ESPECIALIZACION DE X Y RAICES DE POLINOMIOS

### 12.7.1. Especialización de la indeterminada X

Sean $P \in K[X]$ y $\alpha \in K$

***Definición***

Especialización de X por $\alpha$ es el elemento de K

$$P(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \quad \text{si} \quad gP > 0$$

$$P(\alpha) = P \quad \text{si} \quad gP = 0$$

$$P(\alpha) = 0 \quad \text{si} \quad P = \mathbf{0}$$

*Ejemplo 12-13.*

Determinar las especializaciones de X en los siguientes casos

i) $\alpha = \sqrt{2}$ y $P = 2X^4 - X^2 + 1$ en $\mathbf{R}[X]$

Se tiene

$$P(\sqrt{2}) = 2(\sqrt{2})^4 - (\sqrt{2})^2 + 1 = 7$$

ii) $\alpha = 1 + i$ y $P = iX + i$ en $\mathbf{C}[X]$

Resulta

$$P(1+i) = i(1+i) + i = 2i - 1$$

iii) $\alpha = \overline{2}$ y $P = \overline{3}$ en $\mathbf{Z}_5[X]$

Entonces

$$P(\overline{2}) = \overline{3}$$

iv) De modo más general, si $P \in K[X]$, la especialización de X por $\alpha$ define una función de $K[X]$ en sí mismo. Si $P = X^2 - 1$, y $\alpha = X - 1$, entonces

$$P(\alpha) = (X-1)^2 - 1 = X^2 - 2X$$

### 12.7.2. Raíces de polinomios

Sean $P \in K[X]$ y $\alpha \in K$

***Definición***

$\alpha \in K$ es raíz de P si y sólo si la especialización de X por $\alpha$ es 0.

O sea

$$\alpha \text{ es raíz de } P \Leftrightarrow P(\alpha) = 0$$

**Propiedad:** $\alpha$ es raíz de P si y sólo si $X - \alpha$ es divisor de P.

I. $\alpha$ es raíz de P $\Rightarrow X - \alpha | P$

Dividiendo P por $X - \alpha$, se tiene

$$P = (X - \alpha)\,Q + r \qquad (1)$$

Especializando X por $\alpha$ se tiene

$$P(\alpha) = (\alpha - \alpha)\,Q(\alpha) + r = r$$

Y como $\alpha$ es raíx de P, por definición resulta $P(\alpha) = 0 = r$ sustituyendo en (1)

$$P = (X - \alpha)\,Q$$

y en consecuencia

$$X - \alpha | P$$

II. $X - \alpha | P \Rightarrow \alpha$ es raíz de P

Por hipótesis

$$X - \alpha | P$$

Por definición de divisor, $\exists$ Q tal que

$$P = (X - \alpha)\,Q$$

Especializando X por

$$P(\alpha) = (\alpha - \alpha)\,Q(\alpha) = 0$$

Es decir, $\alpha$ es raíz de P.

12.7.3. **Teorema del resto.** El resto de la división de P por $X - \alpha$ es $P(\alpha)$.

Demostración)

Dividiendo P por $X - \alpha$, se tiene

$$P = (X - \alpha)\,Q + r$$

Especializando X por $\alpha$ resulta

$$P(\alpha) = (\alpha - \alpha)\,Q(\alpha) + r$$

O sea

$$r = P(\alpha)$$

Una consecuencia inmediata del teorema del resto es la siguiente

$$X - \alpha | P \Leftrightarrow P(\alpha) = 0$$

***Ejemplo 12-14.***

i ) Determinar si $P = X^n - a^n$ es divisible por $X - a$.
Como $r = P(a) = a^n - a^n = 0$, resulta $X - a | P$.

ii ) Obtener el resto de la división de $P = 3X^2 - 6X + 1$ por $(3X + 6)$.
Dividiendo ambos polinomios por 3, se tienen

$$X^2 - 2X + \frac{1}{3} \quad \text{y} \quad X + 2$$

El resto de su división es

$$r' = (-2)^2 - 2(-2) + \frac{1}{3} = 8 + \frac{1}{3} = \frac{25}{3}$$

De acuerdo con 12.4.3. III.

$$\frac{r}{3} = r'$$

O sea

$$r = 25$$

### 12.7.4. Raíces distintas de $P \in K[X]$

Si $\alpha_1, \alpha_2, \ldots, \alpha_n$ son raíces distintas de $P \in K[X]$, entonces

$$\prod_{i=1}^{n} (X - \alpha_i) | P$$

I. La propiedad es válida para $n = 1$, pues

$$\prod_{i=1}^{1} (X - \alpha_i) = X - \alpha_1 | P \quad \text{ya que } \alpha_1 \text{ es raíz de P.}$$

II. Demostramos ahora

$$\prod_{i=1}^{h} (X - \alpha_i) | P \Rightarrow \prod_{i=1}^{h+1} (X - \alpha_i) | P$$

Por hipótesis y definición de divisor $\exists\, Q$ tal que

$$P = Q \prod_{i=1}^{h} (X - \alpha_i) \qquad (1)$$

El resto de la división de Q por $(X - \alpha_{h+1})$ es $r = Q(\alpha_{h+1})$.
Especializando en (1) X por $\alpha_{h+1}$

$$P(\alpha_{h+1}) = Q(\alpha_{h+1}) \prod_{i=1}^{h} (\alpha_{h+1} - \alpha_i) = 0$$

por ser $\alpha_{h+1}$ raíz de P. Como las raíces son distintas

$$\alpha_{h+1} - \alpha_i \neq 0 \quad \forall i = 1, \ldots, h$$

resulta Q $(\alpha_{h+1}) = 0$

O sea, $r = 0$

Entonces, $X - \alpha_{h+1} | Q \Rightarrow Q = S(X - \alpha_{h+1})$ (2)

De (1) y (2)

$$P = S(X - \alpha_{h+1}) \prod_{i=1}^{h} (X - \alpha_i)$$

y por lo tanto

$$\prod_{i=1}^{h+1} (X - \alpha_i) | P$$

**Consecuencia.** Todo polinomio de grado $n$ en K [X] tiene a lo sumo $n$ raíces distintas.

Demostración)

Sean $\alpha_1, \alpha_2, \ldots, \alpha_m$ todas las raíces distintas de P. Por el teorema anterior se verifica

$$\prod_{i=1}^{m} (X - \alpha_i) | P$$

Entonces

$$P = Q \prod_{i=1}^{m} (X - \alpha_i)$$

Luego

$$n = gP = gQ + m \geqslant m$$

Es decir

$$m \leqslant n$$

## 12.8. RAICES MULTIPLES

Sea $\alpha$ raíz de $P \in K[X]$.

***Definición***

$\alpha$ tiene multiplicidad $p \in \mathbf{N}$ si y sólo si P es múltiplo de $(X - \alpha)^p$ pero no lo es de $(X - \alpha)^{p+1}$

En este caso se dice que $\alpha$ es raíz múltiple de orden $p$.

O sea

$$\alpha \text{ es raíz múltiple de orden } p \in \mathbf{N} \Leftrightarrow (X - \alpha)^p | P \wedge (X - \alpha)^{p+1} \nmid P$$

La definición dada puede traducirse de la siguiente manera

$$\alpha \text{ es raíz múltiple de orden } p \Leftrightarrow P = (X-\alpha)^p\, Q \;\wedge\; Q(\alpha) \neq 0$$

Las raíces de multiplicidad 1 se llaman simples.

Por ejemplo, 0 es raíz doble de $P = X^2$; 1 es raíz triple de $Q = X(X-1)^3$ y 0 es raíz simple.

## 12.9. POLINOMIO DERIVADO Y RAICES MULTIPLES

### 12.9.1. Operador derivado

La función $D : K[X] \to K[X]$

definida por

$$D(P) = D\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=1}^{n} i a_i X^{i-1} = P' \quad \text{si} \quad gP > 0$$

$$D(P) = 0 \quad \text{si} \quad P = \mathbf{0} \;\vee\; gP = 0$$

recibe el nombre de operador derivado en $K[X]$, y la imagen por D de todo polinomio P se llama polinomio derivado de P.

El operador derivado satisface las reglas usuales de la derivación

i ) $(P+Q)' = P' + Q'$

ii ) $(aP)' = aP'$

iii) $(PQ)' = P'Q + PQ'$

iv) $(P^n)' = nP^{n-1}\, P'$

### 12.9.2. Propiedad.

$\alpha \in K$ es raíz múltiple de orden $m > 1$ del polinomio P si y sólo si $\alpha$ es raíz de P y de P'.

I. Sea $\alpha$ raíz de P con multiplicidad $m > 1$. Entonces, por definición 12.8, es

$$P = (X-\alpha)^m\, Q \;\wedge\; Q(\alpha) \neq 0$$

Derivando

$$P' = m\,(X-\alpha)^{m-1}\, Q + (X-\alpha)^m\, Q'$$

Especializando X por $\alpha$ resulta

$$P'(\alpha) = 0 \quad \text{ya que} \quad m > 1$$

O sea, $\alpha$ es raíz de P'.

II. Sea $\alpha$ raíz de P y de P'. Hay que probar que $\alpha$ es raíz de P con multiplicidad mayor que 1.

Por hipótesis

$$P(\alpha)=0 \Rightarrow X-\alpha \mid P \Rightarrow P=(X-\alpha)\,Q \qquad (1)$$

$$P'(\alpha)=0 \Rightarrow X-\alpha \mid P' \Rightarrow P'=(X-\alpha)\,S \qquad (2)$$

Derivando (1)

$$P'=Q+(X-\alpha)\,Q'$$

Sustituyendo en (2)

$$Q+(X-\alpha)\,Q'=(X-\alpha)\,S$$

Entonces

$$Q=(X-\alpha)(S-Q')=(X-\alpha)\,T \qquad (3)$$

De (1) y (3) resulta

$$P=(X-\alpha)^2\,T$$

O sea, $\alpha$ es raíz de P con multiplicidad $m \geqslant 2$.

## 12.10. NUMERO DE RAICES DE POLINOMIOS

Sea $P \in K[X]$ un polinomio de grado $n$, y sean $\alpha_1, \alpha_2, \ldots, \alpha_k$ todas sus raíces distintas con multiplicidades $m_1, m_2, \ldots, m_k$, respectivamente.

**Teorema.** La suma de las multiplicidades de las raíces distintas de todo polinomio de grado $n$ es menor o igual que $n$.

$$\sum_{i=1}^{k} m_i \leqslant gP = n$$

Lo demostramos por inducción sobre $k$.

i ) Sea $k=1$, es decir, que la única raíz es $\alpha_1$ con multiplicidad $m_1$. Entonces, por 12.8. se tiene

$$P=(X-\alpha_1)^{m_1}\,Q \ \wedge \ Q(\alpha_1)\neq 0$$

Luego

$$\sum_{i=1}^{1} m_i = m_1 = g\,(X-\alpha_1)^{m_1} \leqslant m_1+gQ=gP=n$$

ii ) Debemos probar que si la propiedad se cumple para $k=h$, entonces se verifica para $k=h+1$, o sea

$$\sum_{i=1}^{h} m_i \leqslant n \Rightarrow \sum_{i=1}^{h+1} m_i \leqslant n$$

En efecto, siendo $\alpha_1, \alpha_2, \ldots, \alpha_h$ raíces distintas de P con multiplicidades $m_1, m_2, \ldots, m_h$, se tiene

$$P = \overset{h}{\underset{i=1}{\pi}} (X - \alpha_i)^{m_i} . Q \quad y \quad Q(\alpha_i) \neq 0 \text{ para } i = 1, 2, \ldots, h$$

Debe ser Q divisible por $(X - \alpha_{h+1})^{m_{h+1}}$. Sean H y R el cociente y el resto de la división, es decir

$$Q = (X - \alpha_{h+1})^{m_{h+1}} H + R$$

Si $R = \mathbf{0}$, entonces

$$P = \overset{h+1}{\underset{i=1}{\pi}} (X - \alpha_i)^{m_i} H$$

y en consecuencia

$$n = gP = \sum_{i=1}^{h+1} m_i + gH \geqslant \sum_{i=1}^{h+1} m_i$$

Si $R \neq \mathbf{0}$, entonces

$$P = \overset{h+1}{\underset{i=1}{\pi}} (X - \alpha_i)^{m_i} . H + \overset{h}{\underset{i=1}{\pi}} (X - \alpha_i)^{m_i} R$$

Como

$$(X - \alpha_{h+1})^{h+1} | P$$

Resulta

$$(X - \alpha_{h+1})^{h+1} | R \overset{h}{\underset{i=1}{\pi}} (X - \alpha_i)^{m_i}$$

y en consecuencia

$$(X - \alpha_{h+1})^{h+1} | R$$

O sea

$$R = (X - \alpha_{h+1})^{h+1} S$$

Luego

$$P = \overset{h+1}{\underset{i=1}{\pi}} (X - \alpha_i)^{m_i} (H + S) = \overset{h+1}{\underset{i=1}{\pi}} (X - \alpha_i)^{m_i} T$$

Entonces

$$n \doteq gP = \sum_{i=1}^{h+1} m_i + gT \geqslant \sum_{i=1}^{h+1} m_i$$

**Consecuencia.** Todo polinomio de grado $n$ en K [X] tiene, a lo sumo, $n$ raíces.

En efecto, si $\alpha_1, \alpha_2, \ldots, \alpha_k$ son todas las raíces distintas de P con multiplicidades $m_1, m_2, \ldots, m_k$, respectivamente, entonces el número total de raíces es

$$\sum_{i=1}^{k} m_i \leqslant n$$

***Ejemplo 12-15.***

El polinomio $P = X^4 - 4\,X^3 + 5\,X^2 - 4\,X + 4$ en **R** [X] admite la raíz 2, pues $P(2) = 0$.

El polinomio derivado $P' = 4\,X^3 - 12\,X^2 + 10\,X - 4$ es tal que $P'(2) = 0$, y en consecuencia 2 es, al menos, raíz doble de P.

Aplicando reiteradamente la regla de Ruffini

| | | | | | |
|---|---|---|---|---|---|
| | 1 | −4 | 5 | −4 | 4 |
| 2 | | 2 | −4 | 2 | −4 |
| | 1 | −2 | 1 | −2 | 0 |
| 2 | | 2 | 0 | 2 | |
| | 1 | 0 | 1 | 0 | |

Resulta

$$P = (X - 2)^2\,(X^2 + 1)$$

Es decir P admite en **R** [X] la única raíz doble 2, y la forma propuesta es la descomposición factorial de P en **R**.

## 12.11. RAICES DE POLINOMIOS REALES

Sea $P \in \mathbf{R}[X]$, de grado $n$.

**12.11.1. Teorema de Gauss.** Si el polinomio real P, de grado $n$, con coeficientes enteros, admite una raíz racional $\frac{p}{q}$ (siendo $p$ y $q$ coprimos), entonces $p$ es divisor del término independiente y $q$ lo es del coeficiente principal.

Hipótesis) $P = \sum_{i=0}^{n} a_i\,X$ es tal que $a_i \in Z$ y $a_n \neq 0$

$$\frac{p}{q} \in Q \quad \text{es raíz de P} \quad \text{y} \quad \text{m.c.d.}\,(p\,,q) = 1$$

Tesis) $p | a_0 \;\wedge\; q | a_n$

**Demostración)**

Como $\frac{p}{q} \in \mathbf{Q}$ es raíz de P, se verifica

$$P\left(\frac{p}{q}\right) = 0$$

O sea

$$\sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = 0$$

Entonces

$$q^n \sum_{i=0}^{n} a_i \frac{p^i}{q^i} = 0 \Rightarrow \sum_{i=0}^{n} a_i p^i q^{n-i} = 0 \Rightarrow$$

$$\Rightarrow a_0 q^n + p\left(\sum_{i=1}^{n} a_i p^{i-1} q^{n-i}\right) = 0 \Rightarrow$$

$$\Rightarrow a_0 q^n = p\left(-\sum_{i=1}^{n} a_i p^{i-1} q^{n-i}\right) \Rightarrow$$

$$\Rightarrow a_0 q^n = p \,.\, s \quad \text{con} \quad s \in Z \qquad (1)$$

Distinguimos dos casos

i ) $a_0 = 0$ y el teorema se cumple con $p = 0$ y $q = 1$

ii ) $a_0 \neq 0$

Entonces $p \neq 0$, pues si fuera $p = 0$, como $q \neq 0$, por (1) sería $a_0 = 0$, contra lo supuesto.

En este caso, de (1), resulta

$$p | a_0 \, q^n$$

y como $p$ y $q$ son coprimos, se tiene $p | a_0$ por 9-8 ii)

Por otra parte

$$\sum_{i=0}^{n} a_i p^i q^{n-i} = 0 \Rightarrow \left(\sum_{i=0}^{n-1} a_i p^i q^{n-i}\right) + a_n p^n = 0 \Rightarrow$$

$$\Rightarrow a_n p^n = q\left(-\sum_{i=0}^{n-1} a_i p^i q^{n-i-1}\right) \Rightarrow$$

$$\Rightarrow a_n p^n = q \,.\, t \quad \text{con} \quad t \in Z \Rightarrow$$

$$\Rightarrow q | a_n p^n \Rightarrow q | a_n$$

***Ejemplo 12-16.***

Determinar, si existen, las raíces racionales de

$$P = 8 X^3 + 10 X^2 - 11 X + 2$$

Si existen raíces racionales $\frac{p}{q}$, debe ser $p|2 \wedge q|8$

Los divisores de 2 son: 1, −1, 2 y −2.

Los divisores de 8 son: 1, 2, −2, 4, −4, 8 y −8.

De los 10 números racionales, $-2$, $\frac{1}{2}$ y $\frac{1}{4}$ son las raíces de P, y en consecuencia la descomposición factorial es

$$P = 8(X+2)\left(X-\frac{1}{2}\right)\left(X-\frac{1}{4}\right)$$

### 12.11.2. Raíces complejas de polinomios reales

Sea $P \in R[X]$ un polinomio de grado $n$.

**Teorema.** Si un polinomio real admite una raíz compleja, entonces admite a su conjugada.

Hipótesis) $P = \sum_{i=0}^{n} a_i X^i$ es tal que $a_i \in R$ y $z \in C$ es raíz

Tesis) $\bar{z}$ es raíz de P

Demostración)

Debemos probar que

$$P(\bar{z}) = 0$$

Por hipótesis

$$P(z) = 0$$

$$\Downarrow$$

$$\sum_{i=0}^{n} a_i z^i = 0$$

$$\Downarrow$$

$$\overline{\sum_{i=0}^{n} a_i z^i} = \bar{0}$$

$$\Downarrow$$

$$\sum_{i=0}^{n} \overline{a_i z^i} = 0$$ por conjugado de la suma y de 0.

$$\Downarrow$$

$$\sum_{i=0}^{n} \overline{a_i}\, \overline{z^i} = 0$$ por conjugado del producto.

$$\Downarrow$$

$$\sum_{i=0}^{n} a_i (\bar{z})^i = 0$$ por conjugado de una potencia y por ser $a_i \in R$

$$\Downarrow$$

$$P(\bar{z}) = 0$$

$$\Downarrow$$

$\bar{z}$ es raíz de P

*Nota:*

Una consecuencia inmediata de este teorema es que todo polinomio real de grado impar admite una raíz real.

**12.11.3. Teorema fundamental del álgebra.** Todo polinomio real de grado positivo admite una raíz en **C**.

La demostración de este teorema exige recursos no algebraicos y la omitimos.

**12.11.4. Descomposición factorial de polinomios reales**

Sea $P \in R[X]$, de grado $n > 0$.

**Teorema.** Si P es un polinomio real de grado $n \geqslant 1$, entonces existen $n$ complejos $\alpha_1, \alpha_2, \ldots, \alpha_n$, tales que

$$P = a_n \prod_{i=1}^{n} (X - \alpha_i)$$

i ) Si $gP = n = 1$, entonces

$$P = a_1 X + a_0 = a_1 \left( X + \frac{a_0}{a_1} \right) \quad \text{pues } a_1 \neq 0$$

Luego

$$P = a_1 \prod_{i=1}^{1} (X - \alpha_i) \quad \text{donde} \quad \alpha_1 = -\frac{a_0}{a_1}$$

ii ) Suponemos que la propiedad se verifica para $gP = h < n$.

Sea P de grado $h + 1$ y $\alpha_{h+1}$ raíz de P, la cual existe por el teorema fundamental.

Entonces

$$P = (X - \alpha_{h+1})\, Q \qquad (1)$$

siendo $gQ = h$.

Por la hipótesis inductiva se tiene

$$Q = a_{h+1} \prod_{i=1}^{h} (X - \alpha_i)$$

Y sustituyendo en (1)

$$P = a_{h+1} \prod_{i=1}^{h+1} (X - \alpha_i)$$

***Ejemplo 12-17.***

Efectuar la descomposición factorial del polinomio

$$P = \frac{1}{2} X^3 - \frac{3}{2} X^2 + 2X - 1$$

en C [X].

$$P = \frac{1}{2} (X^3 - 3X^2 + 4X - 2)$$

Como $\alpha_1 = 1$ es raíz de

$$Q = X^3 - 3X^2 + 4X - 2$$

entonces $(X - 1)$ es divisor de Q.

Efectuando la división por la regla de Ruffini

| | | | | |
|---|---|---|---|---|
| | 1 | −3 | 4 | −2 |
| 1 | | 1 | −2 | 2 |
| | 1 | −2 | 2 | 0 |

el cociente es

$$S = X^2 - 2X + 2$$

y sus raíces son

$$\alpha_{2,3} = 1 \pm i$$

Luego

$$P = \frac{1}{2} (X - 1)(X - 1 - i)(X - 1 + i)$$

## 12.12. RELACIONES ENTRE RAICES Y COEFICIENTES

Sea $P = \sum_{i=0}^{n} a_i X^i$ (1) un polinomio de grado $n$ en C [X]. Su descomposición factorial es, en consecuencia

$$P = a_n \prod_{i=1}^{n} (X - \alpha_i)$$

Es decir

$$P = a_n (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$$

donde $\alpha_i$ con $i = 1, 2, \dots, n$ son todas sus raíces complejas, simples o múltiples. Efectuando el producto de los polinomios mónicos irreducibles, se tiene

$$\begin{aligned} P = a_n\,[X^n &- (\alpha_1 + \alpha_2 + \ldots + \alpha_n)\,X^{n-1} + \\ &+ (\alpha_1\,\alpha_2 + \alpha_1\,\alpha_3 + \ldots + \alpha_{n-1}\,\alpha_n)\,X^{n-2} - \\ &- (\alpha_1\,\alpha_2\,\alpha_3 + \alpha_1\,\alpha_2\,\alpha_4 + \ldots + \alpha_{n-2}\,\alpha_{n-1}\,\alpha_n)\,X^{n-3} + \ldots + \\ &+ (-1)^n\,\alpha_1\,\alpha_2 \ldots \alpha_n] \qquad (2) \end{aligned}$$

De (1) y (2) resulta

$$-a_n\,(\alpha_1 + \alpha_2 + \ldots + \alpha_n) = a_{n-1}$$
$$a_n\,(\alpha_1\,\alpha_2 + \alpha_1\,\alpha_3 + \ldots + \alpha_{n-1}\,\alpha_n) = a_{n-2}$$
$$-a_n\,(\alpha_1\,\alpha_2\,\alpha_3 + \alpha_1\,\alpha_2\,\alpha_3 + \ldots + \alpha_{n-2}\,\alpha_{n-1}\,\alpha_n) = a_{n-3}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(-1)^n\,a_n\,\alpha_1\,\alpha_2 \ldots \alpha_n = a_0$$

Entonces

$$\alpha_1 + \alpha_2 + \ldots + \alpha_n = -\frac{a_{n-1}}{a_n}$$
$$\alpha_1\,\alpha_2 + \alpha_1\,\alpha_3 + \ldots + \alpha_{n-1}\,\alpha_n = \frac{a_{n-2}}{a_n}$$
$$\alpha_1\,\alpha_2\,\alpha_3 + \ldots + \alpha_{n-2}\,\alpha_{n-1}\,\alpha_n = -\frac{a_{n-3}}{a_n}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\alpha_1\,\alpha_2\,\alpha_3 \ldots \alpha_{n-1}\,\alpha_n = (-1)^n\,\frac{a_0}{a_n}$$

O sea

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}$$
$$\sum_{i<j}^{n} \alpha_i\,\alpha_j = \frac{a_{n-2}}{a_n}$$
$$\sum_{i<j<k}^{n} \alpha_i\,\alpha_j\,\alpha_k = -\frac{a_{n-3}}{a_n}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\prod_{i=1}^{n} \alpha_i = (-1)^n\,\frac{a_0}{a_n}$$

Expresando

$$P = a_n\,X^n + a_{n-1}\,X^{n-1} + \ldots + a_1\,X + a_0$$

las relaciones anteriores se traducen en

i ) La suma de las raíces es igual al segundo coeficiente cambiado de signo, dividido por el coeficiente principal.

ii ) La suma de los productos binarios de las raíces es igual al tercer coeficiente dividido por el coeficiente principal.

Las mismas reglas valen para las sumas de productos ternarios, cuaternarios, etcétera, con signos − o +, alternativamente.

El producto de las $n$ raíces es igual al término independiente dividido por el coeficiente principal, con signo + o −, según que $n$ sea par o impar, respectivamente.

*Ejemplo 12-18.*

Determinar el polinomio mónico de grado 3 cuyas raíces son

$$\alpha_1 = 1 \quad , \quad \alpha_2 = -1 \quad , \quad \alpha_3 = 2$$

Hay que obtener $a_2$ . $a_1$ y $a_0$ tales que

$$P = X^3 + a_2 X^2 + a_1 X + a_0$$

Como

$$\alpha_1 + \alpha_2 + \alpha_3 = 2 = -\frac{a_2}{a_3} = -a_2$$

$$\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 = -1 = \frac{a_1}{a_3} = a_1$$

$$\alpha_1 \alpha_2 \alpha_3 = -2 = -\frac{a_0}{a_3} = -a_0$$

Se tiene

$$a_2 = -2 \quad , \quad a_1 = -1 \quad , \quad a_0 = 2$$

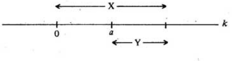
Luego

$$P = X^3 - 2X^2 - X + 2$$

## 12.13. FORMULA DE TAYLOR Y METODO DE HORNER

Sea $P = \sum_{i=0}^{n} a_i X^i$ en K [X] un polinomio de grado positivo.

Pensando P como una función de K en K respecto de la especialización de X, si efectuamos una traslación definida por $a \in K$, al referir a P respecto del nuevo origen, la indeterminada Y está vinculada con X mediante $X = Y + a$




O sea $Y = X - a$
Entonces se tiene

$$P = \sum_{i=0}^{n} b_i (X-a)^i$$

donde P queda expresado en potencias de $X - a = Y$, y cuyos coeficientes $b_i$ serán determinados a continuación.

### 12.13.1. Fórmula de Taylor

A partir del polinomio $P = \sum_{i=0}^{n} b_i (X-a)^i$ (1) de grado $n > 0$, determinamos las $n$ derivadas sucesivas:

$$P' = \sum_{i=1}^{n} i\, b_i (X-a)^{i-1}$$

$$P'' = \sum_{i=2}^{n} i\,(i-1)(X-a)^{i-2}$$

$$P''' = \sum_{i=3}^{n} i\,(i-1)(i-2)(X-a)^{i-3}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$P^{(n-1)} = \sum_{i=n-1}^{n} i\,(i-1)(i-2)\,\ldots\,[i-(n-2)](X-a)^{i-(n-1)}$$

$$P^{(n)} = \sum_{i=n}^{n} i\,(i-1)(i-2)\,\ldots\,[i-(n-1)](X-a)^{i-n}$$

Especializando X por $a$ en P y en las $n$ derivadas, se tiene

$$P\,(a) = b_0$$

$$P'\,(a) = 1\,.\,b_1 = 1!\,b_1$$

$$P''\,(a) = 2\,.\,1\,.\,b_2 = 2!\,b_2$$

$$P'''(a) = 3\,.\,2\,.\,1\,.\,b_3 = 3!\,b_3$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$P^{(n)}(a) = n!\,b_n$$

Entonces

$$b_0 = P(a)$$
$$b_1 = \frac{1}{1!} P'(a)$$
$$b_2 = \frac{1}{2!} P''(a)$$
$$\dots\dots\dots\dots\dots\dots$$
$$b_n = \frac{1}{n!} P^{(n)}(a)$$

Y sustituyendo en (1) resulta la fórmula de Taylor

$$P = P(a) + \sum_{i=1}^{n} \frac{P^{(i)}(a)}{i!} (X-a)^i$$

Si convenimos en llamar a P (*a*), la derivada de orden o de P en *a*, podemos escribir

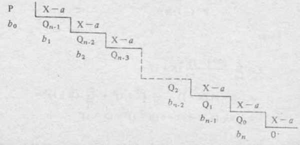
$$P(a) = \frac{P^{(o)}(a)}{o!}$$

Y la fórmula anterior se expresa así

$$P = \sum_{i=0}^{n} \frac{P^{(i)}(a)}{i!} (X-a)^i$$

## 12.13.2. Método de Horner

Para obtener los coeficientes $b_i$ de la fórmula ( ) efectuamos las $n+1$ divisiones sucesivas siguientes, hasta obtener un cociente nulo




donde $gQ_i = i$, $\forall i = 0, 1, \dots, n-1$

Por el algoritmo de la división se tiene

$$\begin{aligned} P &= b_0 + (X-a)\,Q_{n-1} = b_0 + (X-a)\,[b_1 + (X-a)\,Q_{n-2}] = \\ &= b_0 + b_1\,(X-a) + (X-a)^2\,Q_{n-2} = \\ &= b_0 + b_1\,(X-a) + b_2\,(X-a)^2 + (X-a)^3\,Q_{n-3} = \\ &= \ldots = b_0 + b_1\,(X-a) + b_2\,(X-a)^2 + \ldots + b_n\,(X-a)^n \end{aligned}$$

cuyos coeficientes son los sucesivos restos que resultan de las divisiones sucesivas indicadas.

***Ejemplo 12-19.***

Expresar el polinomio $P = X^3 - 3\,X^2 + 2\,X + 1$ en potencias de $X + 1$ utilizando los métodos anteriores.

i ) Fórmula de Taylor. Obtenemos los polinomios derivados

$$\begin{aligned} P' &= 3\,X^2 - 6\,X + 2 \\ P'' &= 6\,X - 6 \\ P''' &= 6 \end{aligned}$$

Especializamos X por $-1$

$$\begin{aligned} P(-1) &= -1 - 3 - 2 + 1 = -5 \\ P'(-1) &= 3 + 6 + 2 = 11 \\ P''(-1) &= -6 - 6 = -12 \\ P'''(-1) &= 6 \end{aligned}$$

Luego

$$\begin{aligned} P &= \sum_{i=0}^{3} \frac{P^{(i)}(-1)}{i!}\,(X+1)^i = \\ &= -5 + 11\,(X+1) - \frac{12}{2!}\,(X+1)^2 + \frac{6}{3!}\,(X+1)^3 = \\ &= -5 + 11\,(X+1) - 6\,(X+1)^2 + (X+1)^3 \end{aligned}$$

ii ) Método de Horner. Efectuamos las divisiones indicadas en 12.13.2. mediante la regla de Ruffini

| | | | | |
|---|---|---|---|---|
| | 1 | −3 | 2 | 1 |
| −1 | 1 | −1 | 4 | −6 |
| | 1 | −4 | 6 | −5 |
| −1 | 1 | −1 | 5 | |
| | 1 | −5 | 11 | |
| −1 | | −1 | | |
| | 1 | −6 | | |

y los coeficientes son $b_0 = -5$, $b_1 = 11$, $b_2 = -6$ y $b_3 = 1$.
Se tiene

$$P = -5 + 11(X+1) - 6(X+1)^2 + (X+1)^3$$

## TRABAJO PRACTICO XII

*12-20.* Determinar $a$, $b$ y $c$ en **R**, de modo que

i ) $9X^2 - 16X + 4 = a(X-1)(X-2) + bX(X-2) + cX(X-1)$

ii ) $X + 2 = a(X^2 + X + 1) + (bX + c)(X-1)$

*12-21.* Dados en $\mathbf{Z}_6$ [X] los polinomios

$$P = \overline{2}X^4 + X^3 + \overline{4}X + \overline{3}$$
$$Q = \overline{3}X^2 + \overline{5}X + \overline{1}$$

Determinar

i ) $\overline{2}P - Q$

ii ) $PQ$

iii) $P^2 + Q$

iv) el grado de $XP + \overline{2}Q$

*12-22.* Obtener el número de polinomios en $\mathbf{Z}[X]$ de grado menor que 4 con coeficientes $a_i$ tales que $|a_i - 1| \leqslant 3$

*12-23.* Determinar si existen polinomios $A \in \mathbf{R}[X]$ de grado positivo, tales que $A^2 - A = \mathbf{0}$.

*12-24.* Obtener el cociente y el resto de la división de A por B, pertenecientes a $\mathbf{Q}[X]$, en los siguientes casos:

i ) $A = -X$ $\qquad B = \frac{1}{2}X - 1$

ii ) $A = X^4 - X^2 + 2$ $\qquad B = -X^4 + 2X - 1$

iii) $A = 2X^2 - 1$ $\qquad B = X^3 - X$

*12-25.* Dados $A = X^3 + 2mX + m$ y $B = X^2 + mX - 1$ en $\mathbf{R}[X]$, determinar $m$ para que A sea divisible por B.

*12-26.* Mediante la regla de Ruffini, determinar el cociente y el resto de la división de A por B en cada uno de los siguientes casos

i ) $A = -aX^3 + a^3X - 1$ $\qquad B = X - a$

ii ) $A = \overline{3}X^4 + X^2 + \overline{4}X + \overline{2}$ $\qquad B = X + \overline{2}$ en $\mathbf{Z}_5$ [X]

iii) $A = i X^4 - 2 X^2 + i$ $\qquad B = X + i$ en $\mathbf{C}[X]$

iv) $A = 3 X^3 - 6 X + 1$ $\qquad B = 3 X - 9$

*12-27.* Determinar el m.c.d. de los pares de polinomios que se indican

i ) $A = X^4 + X^3 - X^2 + X - 2$ y $B = X^4 + X^3 - 3 X^2 - X + 2$

ii ) $A = X^4 - 16$ y $B = X^2 + 4$

iii) $A = X^{11} - 1$ y $B = X^{33} - 1$

iv) $A = X^3 + 2 X^2 - X - 2$ y $B = X^4 + 2 X^2 - 3$

*12-28.* Sean P y Q en K [X] y $a \in$ K. Demostrar que $P \cdot Q(a) - P(a) \cdot Q$ es múltiplo de $X - a$.

*12-29.* Realizar la descomposición factorial de $P = X^3 + 4 X^2 - 4 X - 16$ en $\mathbf{Q}[X]$, $\mathbf{R}[X]$ y $\mathbf{C}[X]$.

*12-30.* Verificar que $P = X^4 - 5 X^2 + 6$ carece de raíces racionales.

*12-31.* Obtener todas las raíces de $P = X^4 - 10 X + 1$

*12-32.* El polinomio $P = X^3 + 2 X^2 - 4 X - 8$ admite una raíz doble. Obtener la descomposición factorial en $\mathbf{Q}[X]$.

*12-33.* Expresar en la forma $X^4 + \sum_{i=3}^{0} a_i X^i$ el polinomio $P = \prod_{i=1}^{4} (X - \alpha_i)$ tal que $\alpha_i \in \mathbf{R}$ para $i = 1, 2, 3, 4$

*12-34.* Determinar el polinomio mónico de grado 4, cuyas raíces son $-2, -1, 1$ y $2$.

*12-35.* Investigar si los siguientes polinomios son irreducibles en $\mathbf{Q}[X]$ y en $\mathbf{R}[X]$

i ) $A = X^3 - 3$

ii ) $B = 5 X^2 + 4$

iii) $C = X^6 - 1$

*12-36.* Demostrar que $P = \sum_{i=0}^{2} a_i X^i$ es irreducible en $\mathbf{R}[X]$ si y sólo si $\Delta = a_1^2 - 4 a_0 a_2 < 0$.

*12-37.* Proponer un polinomio irreducible en $\mathbf{Q}[X]$ del tipo $a X^2 + b X + c$, tal que $b^2 - 4 ac \geq 0$.

*12-38.* Determinar en $\mathbf{Z}_5[X]$ un polinomio P de grado 2, tal que

$$P(\overline{1}) = \overline{3} \quad , \quad P(\overline{3}) = \overline{0} \quad y \quad P(\overline{2}) = \overline{1}.$$

*12-39.* Sea $B \neq 0$ en K [X]. En [X] se define la relación de congruencia módulo B mediante

$$A \sim A' \Leftrightarrow B | A - A'$$

Demostrar que tal relación es de equivalencia y determinar las clases de equivalencia.

*12-40.* Demostrar que la congruencia módulo $B \neq 0$ en $K[X]$ es compatible con la suma y el producto.

*12-41.* Sean A y B en $K[X]$. Demostrar que

$$I = \{ SA + TB \, / \, S \text{ y } T \in K[X] \}$$

es un ideal de $K[X]$.

*12-42.* Demostrar que la intersección de toda familia de ideales de $K[X]$ es un ideal.

*12-43.* Demostrar que el ideal generado por $A_1$ y $A_2$ en $K[X]$ es igual a la intersección de todos los ideales que contienen a $A_1$ y $A_2$.

*12-44.* Determinar todas las raíces de las siguientes ecuaciones

i ) $X^4 + 16\,i = 0$

ii ) $X^3 + X^2 + X + 1 = 0$

iii) $i\,X^3 + 1 = 0$

*12-45.* Dado $P = 8\,m\,X^2 + 7\,(m-1)\,X + 1$ con $m \neq 0$, determinar $m$ en los siguientes casos

i ) Las raíces son opuestas.

ii ) Las raíces son recíprocas.

iii) Las raíces son reales e iguales.

*12-46.* Resolver las siguientes ecuaciones

i ) $X^3 + 2\,X^2 + 3\,X + 2 = 0$ siendo $\alpha_1 + \alpha_2 - \alpha_3 = 0$

ii ) $2\,X^3 - X^2 - 5\,X - 2 = 0$ siendo $\alpha_1\,\alpha_2 + 1 = 0$

*12-47.* Resolver las siguientes ecuaciones

i ) $ab\,X - b\,X\,(a + b + X) = a\,X\,(a + b + X) + ab\,(a + b + X)$

ii ) $X^8 + 2\,X^4 + 1 = 0$

*12-48.* Dada la ecuación $X^3 - 7\,X + m = 0$, determinar $m$ para que $\alpha_1 - 2\,\alpha_2 = 0$.

*12-49.* Determinar la suma de los cuadrados de las raíces de la ecuación

$$X^4 - 3\,X^3 + \frac{5}{2}\,X^2 - \frac{7}{2}\,X + \frac{1}{2} = 0$$

*12-50.* Dado $P = X^3 - 3\,X^2 + 2\,X$ en $\mathbf{R}[X]$, determinar el polinomio cuyas raíces exceden en 3 a las anteriores.

## BIBLIOGRAFIA


✓ Alexandroff P. S.: *Introducción a la Teoría de Grupos.* Editorial Universitaria de Buenos Aires, 1965.

✓ Apóstol T. M.: *Análisis Matemático.* Editorial Reverté S.A., Barcelona, 1960.

Balanzat M.: *El Número Natural y sus Generalizaciones.* Universidad Nacional de Cuyo, 1953.

✓ Birkhoff-Mac Lane: *Algebra Moderna.* Editorial Teide, Barcelona, 1964.

✓ Bosch J.: *Introducción al Simbolismo Lógico.* Editorial Universitaria de Buenos Aires, 1965.

✓ Copi, I.: *Introducción a la Lógica.* Editorial Universitaria de Buenos Aires, 1962.

✓ Cotlar-Sadosky: *Introducción al Algebra.* Editorial Universitaria de Buenos Aires, 1962.

✓ Chevalley C.: *Fundamental Concepts of Algebra.* Academic Press Inc., Publishers, New York, 1956.

✓ Dieudonné J.: *Fundamentos de Análisis Moderno.* Editorial Reverté S.A., Barcelona, 1966.

✓ Faure-Kaufmann-Denis: *Matemática Moderna.* Editorial Paraninfo, Barcelona, 1966.

✓ Gentile E. R.: *Estructuras Algebraicas.* The Pan American Union, Washington, D.C., 1967.

✓ Gentile E. R.: *Notas de Algebra.* CEFMYN, Buenos Aires, 1964.

✓ Hernández, Rojo, Rabuffetti: *Conceptos Básicos de Matemática Moderna.* Editorial Códex, Buenos Aires, 1966.

Hu S. T.: *Elements of Modern Algebra.* Holden-Day, California, 1965.

✓ Lentin-Rivaud: *Lecons d'Algebra Moderne.* Libraire Vuibert, París, 1961.

Lipschutz S.: *Theory and Problems of Finite Mathematics.* Schaum Publishing CO., New York, 1966.

✓ Lipschutz S.: *Theory and Problems of Set Theory* Schaum Publisihing CO., New York, 1964.

✓Natanson I. P.: *Theory of Functions of a Real Variable.* Frederick Ungar Publishing CO., New York, 1964.

✓Oubiña L.: *Introducción a la Teoría de Conjuntos.* Editorial Universitaria de Buenos Aires, 1965.

✓Rey Pastor-Pi Calleja-Trejo: *Análisis Matemático I.* Editorial Kapelusz, Buenos Aires, 1961.

✓Rudin W.: *Principles of Mathematical Analysis.* Mac Graw-Hill Book Company, New York, 1964.

✓Simmons G. F.: *Introduction to Topology and Modern Analysis.* Mac Graw-Hill Book Company, Inc., New York, 1963.

✓Trejo C.: *El Concepto de Número.* The Pan American Union, Washington, D.C., 1968.

✓Tucker H. G.: *Introducción a la Teoría Matemática de las Probabilidades y a la Estadística.* Editorial Vicens Vives, Barcelona, 1966.

## RESPUESTAS A LOS TRABAJOS PRACTICOS

# TRABAJO PRACTICO I

*1-17.* • Mis maestros hacen que todas las lecciones sean aburridas y no aceptan las respuestas que no figuran en los libros.
- Aceptan las respuestas que no figuran en los libros o imponen un cúmulo de normas estúpidas.
- Si mis maestros hacen que todas las lecciones sean aburridas y no aceptan las respuestas que no figuran en los libros, entonces imponen un cúmulo de normas estúpidas.

*1-18.* La proposición compuesta es la conjunción de 8 proposiciones simples:

$$p_1 \wedge p_2 \wedge \ldots \wedge p_8$$

donde $p_1$: "la chatura de ciertas disciplinas escolares se trasmite a los maestros", etcétera.

*1-19.* Adoptando la combinación de valores de verdad que figura en el texto, los renglones para las tablas propuestas son:

i ) V F V V V V V V    ii ) V V V V

*1-20.* • Mis maestros hacen que algunas lecciones no sean aburridas.
- Aceptan las respuestas que no figuran en los libros.
- No imponen un cúmulo de normas estúpidas.

*1-21.* i ) $\sim p \wedge q$. Su negación equivale a $p \vee \sim q$, y la retraducción es: "es justa o no mantiene el orden".

ii ) $p \wedge q$ ; $\sim p \vee \sim q$; "los alumnos no conocen a los simuladores o no los desprecian".

iii) $p \Rightarrow q$ ; $p \wedge \sim q$; "los alumnos conocen a los simuladores y no los desprecian".

*1-22.* i ) sí.  ii ) sí.  iii) no.  iv) sí.

*1-23.* i ) $p \wedge q$.  ii ) $\sim p \wedge (q \vee \sim q)$.

*1-24.* F.

*1-25.* i ) sí; V.  ii ) sí; F.  iii) sí; V.  iv) no.

*1-26.* i ) V.  ~~ii) V.~~  iii) F.

*1-27.* i ) $\forall x : \sim P(x) \wedge Q(x)$ ii ) $\exists x / P(x) \wedge \sim Q(x)$. iii) $\exists x / \forall y : xy \neq 0$

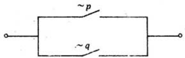
*1-28.* Utilizar la ley del silogismo hipotético.

*1-29.* i ) $\forall x \in \mathbf{R} : x^2 > 2$; $\exists x \in \mathbf{R} / x^2 \leqslant 2$; existe algún número real cuyo cuadrado es menor o igual que 2.

ii ) $\exists x \in \mathbf{Z} / x^3 + 1 = (x+1)^3$; $\forall x \in \mathbf{Z}: x^3 + 1 \neq (x+1)^3$; todo número entero es tal que su cubo aumentado en uno, es distinto del cubo del siguiente.

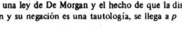
iii) $\forall x : P(x) \Rightarrow Q(x)$ ; $\exists x / P(x) \wedge \sim Q(x)$; existen personas que estudian y no triunfan.

*1-30.* Utilizando leyes lógicas, se llega a la proposición equivalente $\sim p \vee \sim q$, cuyo circuito es




*1-31.* i ) $[(p \wedge q) \vee (\sim p \wedge \sim q) \vee q] \wedge p$

ii ) Utilizando una ley de De Morgan y el hecho de que la disyunción entre una proposición y su negación es una tautología, se llega a $p \wedge q$, cuyo circuito es




*1-32.* $\forall x \in \mathbf{Z} : x$ es impar $\Rightarrow x^2$ es impar.

Contrarrecíproco: si el cuadrado de un entero es par, entonces dicho entero es par.

Contrario: Si un entero es par, entonces su cuadrado es par.

Recíproco: Si el cuadrado de un entero es impar, entonces dicho entero es impar. Para demostrar el teorema contrarrecíproco, considerar $x = x^2 - x(x-1)$.

*1-33.* Suponer que $a$ es par o que $b$ es par; se llega a que $ab$ es par.

*1-34.* De las dos primeras resulta $p \vee r$; considerando esta y la tercera proposición, por ser ambas verdaderas, resulta la verdad de $p$.

*1-35.* De la verdad de las dos primeras se infiere la verdad de $r$, y por la ley del modus ponens, resulta la verdad de $s$.

*1-36.* La forma simbólica del razonamiento es

$$\begin{array}{l} \sim p \Rightarrow r \wedge s \\ \sim r \wedge s \\ \hline p \end{array}$$

La validez se justifica teniendo en cuenta la equivalencia entre una implicación y la disyunción entre la negación del antecedente, y el consecuente.

## TRABAJO PRACTICO II

*2-34.* $S = \{(1,1,1), (1,1,0), (1,0,1), (0,1,1), (1,0,0), (0,1,0), (0,01), (0,0,0)\}$

*2-35.* $S_1 = \{(1,1,1), (1,1,0), (1,0,1), (0,1,1)\}$

$S_2 = S_1$

$S_3 = \{(1,1,1), (0,0,0)\}$

*2-36.* $S_2^c = \{(0,1,0), (1,0,0), (0,01), (0,0,0)\}$

$S_2 - S_3 = \{(1,1,0), (1,0,1), (0,1,1)\}$

$S_1 \cap S_3 = \{(1,1,1)\}$

$(S_2 \cup S_3) \cap S_1 = S_1$

*2-37.* $A = \{-3, -2, -1, 0, 1, 2, 3\}$ y $B = \{-2, -1, 0, 1, 2\}$

$A \cap B = B$, $A \cup B = A$, $A - B = \{-3, 3\}$, $B - A = \phi$, $A \Delta B = A - B$

*2-38.* $A = \left[-\frac{3}{2}, \frac{5}{2}\right]$ y $B = \left[-\frac{1}{2}, \frac{5}{2}\right]$ son dos intervalos cerrados reales.

$A \cap B = B$; $A \cup B = A$; $B^c = \mathbf{R} - B = \left(-\infty, -\frac{1}{2}\right) \cup \left(\frac{5}{2}, \infty\right)$

*2-39.* $A = \{-1, 1\}$ y $B = [-1, 1]$.

$A \cap B = A$, $(A \cup B)^c = B^c = \mathbf{R} - B = \{x \in \mathbf{R} / |x| > 1\} = (-\infty, -1) \cup (1, \infty)$

*2-40.* $A \cup B = \{-6, -3, -2, -1, 0, 1, 2, 3, 6\}$

$A \cap B = \{-3, -2, -1, 1, 2, 3\}$, $A - B = \{0\}$, $B - A = \{-6, 6\}$,

$A \Delta B = \{-6, 0, 6\}$

*2-41.* $\phi$, $\{(0,0)\}$, $\{(1,0)\}$, A

*2-42.* $A^2 = \{(a,a), (a,b), (b,a), (b,b)\}$, los elementos de $P(A^2)$ son: $\phi$, $\{(a,a)\}$

$\{(a,b)\}$, $\{(b,a)\}$, $\{(b,b)\}$, $\{(a,a), (a,b)\}$, $\{(a,a), (b,a)\}$,

$\{(a,a), (b,b)\}$, $\{(a,b), (b,a)\}$, $\{(a,b), (b,b)\}$, $\{(b,a), (b,b)\}$,

$\{(a,a),(a,b),(b,a)\}$, $\{(a,a),(a,b),(b,b)\}$, $\{(a,b),(b,a),(b,b)\}$,
$\{(a,a),(b,a),(b,b)\}$, $A^2$.

*2-43.* i ) $x \in A \cap B \Rightarrow x \in A \ \wedge \ x \in B \Rightarrow x \in A$. Luego, $A \cap B \subset A$.
Usar el mismo procedimiento para demostrar $A \subset A \cup B$.

*2-44.* Considerar $x \in A$, utilizar la hipótesis y la definición de intersección.

*2-45.* Sea $x \in A \cup B \Rightarrow x \in A \ \vee \ x \in B \Rightarrow x \in C \ \vee \ x \in C \Rightarrow x \in C$.

*2-46.* En el texto está demostrado: $\phi \subset A$, y como por hipótesis $A \subset \phi$, resulta $A = \phi$, por definición de igualdad.

*2-47.* Considerar $A - (A \cap B)$, tener en cuenta que la diferencia entre dos conjuntos es igual a la intersección del primero con el complementario del segundo, utilizar una ley de De Morgan y la distributividad de la intersección respecto de la unión, para obtener $A - B$. El mismo procedimiento se sigue para probar $(A \cup B) - - B = A - B$.

*2-48.* Se aplica el mismo método que en el ejercicio anterior.

*2-49.* $(A \cap B) - C = (A \cap B) \cap C^c = A \cap B \cap C^c \cap C^c = (A \cap C^c) \cap (B \cap C^c) =$
$= (A - C) \cap (B - C)$.

*2-50.* $(A - B) - C = (A \cap B^c) \cap C^c = A \cap (B^c \cap C^c) = A \cap (B \cup C)^c = A - (B \cup C)$.

*2-51.* $A - (B - C) = A \cap (B \cap C^c)^c = A \cap (B^c \cup C) = (A \cap B^c) \cup (A \cap C) =$
$= (A - B) \cup (A \cap C)$.

*2-52.* Expresando en términos de intersecciones ambos miembros de la inclusión, hay que demostrar

$$A \cap B^c \cap C^c \subset A \cap (B^c \cup C)$$

Sea $x \in A \cap B^c \cap C^c \Rightarrow x \in A \ \wedge \ x \in B^c \Rightarrow x \in A \ \wedge \ x \in B^c \cup C \Rightarrow x \in A \cap (B^c \cup C)$

*2-53.* $A \cup (B - C) = A \cup (B \cap C^c) = (A \cup B) \cap (A \cup C^c) =$
$= (A \cup B) \cap (C \cap A^c)^c = (A \cup B) - (C - A)$.

*2-54.* $(A \cap B) \cup (A \cap B^c) = A \cap (B \cup B^c) = A \cap U = A$.

*2-55.* Como $(A - B) \cup B = (A \cap B^c) \cup B = (A \cup B) \cap (B^c \cup B) = (A \cup B) \cap U =$
$= A \cup B$, hay que probar $B \subset A \Leftrightarrow A \cup B = A$, lo que está realizado en el texto.

*2-56.* Está demostrado en el ejercicio anterior.

*2-57.* $A \Delta B = \phi \Leftrightarrow (A - B) \cup (B - A) = \phi \Leftrightarrow A - B = \phi \ \wedge \ B - A = \phi \Leftrightarrow$
$\Leftrightarrow A \subset B \ \wedge \ B \subset A \Leftrightarrow A = B$

*2-58.* $A \neq \phi \ \wedge \ B \neq \phi \Leftrightarrow \exists\, x \in A \ \wedge \ \exists\, y \in B \Leftrightarrow \exists\, (x,y) \in A \times B \Leftrightarrow A \times B \neq \phi$.
Luego $A \times B = \phi \Leftrightarrow A = \phi \ \vee \ B = \phi$.

*2-59.* i ) $(x,y) \in A \times C \Rightarrow x \in A \ \wedge \ y \in C \Rightarrow x \in B \ \wedge \ y \in D \Rightarrow (x,y) \in B \times D$
ii ) Sean $x \in A \ \wedge \ y \in C \Rightarrow (x,y) \in A \times C \Rightarrow (x,y) \in B \times D \Rightarrow$
$\Rightarrow x \in B \ \wedge \ y \in D.$

*2-60.* $(x,y) \in (A \cap B) \times C \Rightarrow x \in A \ \wedge \ x \in B \ \wedge \ y \in C \Rightarrow (x \in A \ \wedge \ y \in C) \ \wedge$
$\wedge \ (x \in B \ \wedge \ y \in C) \Rightarrow (x,y) \in A \times C \ \wedge \ (x,y) \in B \times C \Rightarrow$
$\Rightarrow (x,y) \in (A \times C) \cap (B \times C).$

*2-61.* $(x,y) \in (A - B) \times C \Leftrightarrow x \in A \ \wedge \ x \notin B \ \wedge \ y \in C \Leftrightarrow (x \in A \ \wedge \ y \in C) \ \wedge$
$\wedge \ (x \notin B \ \vee \ y \notin C) \Leftrightarrow (x,y) \in A \times C \ \wedge \ (x,y) \notin B \times C \Leftrightarrow$
$\Leftrightarrow (x,y) \in (A \times C) - (B \times C).$

*2-62.* i ) $x \in A \cup C \Rightarrow x \in A \ \vee \ x \in C \Rightarrow x \in B \ \vee \ x \in D \Rightarrow x \in B \cup D$
ii ) Seguir el mismo procedimiento.

*2-63.* i ) $x \in A \Rightarrow x \in B \ \wedge \ x \in C \Rightarrow x \in B \cap C$
ii) $x \in A \Rightarrow x \in B \cap C \Rightarrow x \in B \ \wedge \ x \in C$

*2-64.* Se sigue el esquema del ejercicio anterior.

*2-65.* $x \in A \Leftrightarrow x \in A \ \wedge \ x \notin B \Leftrightarrow x \in C \ \wedge \ x \notin B \Leftrightarrow x \in C - B.$

*2-66.* i ) $x \in U^c \Leftrightarrow x \in U^c \ \wedge \ x \in U \Leftrightarrow x \in U^c \cap U \Leftrightarrow x \in \phi$
ii ) $U = (U^c)^c = \phi^c$
iii) $A \cap A^c = A - A = \phi$
iv) $A \cup A^c = (A^c \cap A)^c = \phi^c = U$

*2-67.* $x \in B \Leftrightarrow x \notin A \Leftrightarrow x \in A^c$

*2-68.* i ) $A - (A - B) = A \cap (A \cap B^c)^c = A \cap (A^c \cup B) =$
$= (A \cap A^c) \cup (A \cap B) = \phi \cup (A \cap B) = A \cap B.$
ii ) $A \cup (B - A) = A \cup (B \cap A^c) = (A \cup B) \cap (A \cup A^c) = (A \cup B) \cap U = A \cup B.$

*2-69.* i ) $x \in A^c \Rightarrow x \notin A \Rightarrow x \in B$
ii ) Se sabe que $A \cup B \subset U$. Además
$x \in U \Rightarrow x \in A \ \vee \ x \in A^c \Rightarrow x \in A \ \vee \ x \in B \Rightarrow x \in A \cup B.$

*2-70.* i ) $x \in A \cap B \Rightarrow x \in A \ \wedge \ x \in B \Rightarrow x \in B^c \ \wedge \ x \in B \Rightarrow x \in \phi$
Luego $A \cap B \subset \phi$ y como $\phi \subset A \cap B$, resulta $A \cap B = \phi$.
ii ) $x \in A \Rightarrow x \notin B \Rightarrow x \in B^c.$

*2-71.* $c\,(A \cup B \cup C) = c\,(A) + c\,(B \cup C) - c\,[A \cap (B \cup C)] =$
$= c\,(A) + c\,(B) + c\,(C) - c\,(B \cap C) - c\,[(A \cap B) \cup (A \cap C)] =$
$= c\,(A) + c\,(B) + c\,(C) - c\,(B \cap C) - c\,(A \cap B) - c\,(A \cap C) + c\,(A \cap B \cap C)$

*2-72.* a) $\phi \in \mathcal{A} \Rightarrow \phi^c \in \mathcal{A} \Rightarrow U \in \mathcal{A}$
b) $A_i \in \mathcal{A} \Rightarrow A_i^c \in \mathcal{A} \Rightarrow \bigcup_{i \in I} A_i^c \in \mathcal{A} \Rightarrow \left(\bigcup_{i \in I} A_i^c\right)^c \in \mathcal{A} \Rightarrow \bigcap_{i \in I} A_i \in \mathcal{A}.$

**2-73.** i ) $A \in \mathcal{A} \cap \mathcal{B} \Rightarrow A \in \mathcal{A} \ \wedge \ A \in \mathcal{B} \Rightarrow A^c \in \mathcal{A} \ \wedge \ A^c \in \mathcal{B} \Rightarrow A^c \in \mathcal{A} \cap \mathcal{B}$.

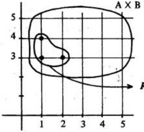
ii ) $A_i \in \mathcal{A} \cap \mathcal{B} \Rightarrow A_i \in \mathcal{A} \ \wedge \ A_i \in \mathcal{B} \Rightarrow \bigcup_{i \in I} A_i \in \mathcal{A} \ \wedge \ \bigcup_{i \in I} A_i \in \mathcal{B} \Rightarrow$
$\Rightarrow \bigcup_{i \in I} A_i \in \mathcal{A} \cap \mathcal{B}$.

iii) $\phi \in \mathcal{A} \ \wedge \ \phi \in \mathcal{B} \Rightarrow \phi \in \mathcal{A} \cap \mathcal{B}$.

## TRABAJO PRACTICO III

*3-19.* i ) $R = \{(1,3), (1,4), (2,3)\}$

ii )




iii) $R^{-1} = \{(3,1), (4,1), (3,2)\}$

*3-20.* i ) $R = \{(1,1), (2,4), (4,16)\}$ $S = \{(4,2), (16,8), (6,3)\}$

ii ) $S \circ R = \{(2,2), (4,8)\}$

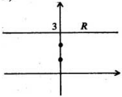
iii) $D_R = \{1, 2, 4\}$ $I_R = \{1, 4, 16\}$

$D_S = \{4, 6, 16\}$ $I_S = \{2, 3, 8\}$

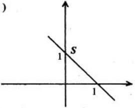
$D_{S \circ R} = \{2, 4\}$ $I_{S \circ R} = \{2, 8\}$

*3-21.*

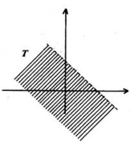
i )




ii )



iii)




*3-22.* $R$ es reflexiva, simétrica y transitiva

*3-23.* a) Reflexividad.

$(x,y) \in \mathbf{R}^2 \Rightarrow y = y \Rightarrow (x,y) \sim (x,y)$

b) Simetría.

$(x,y) \sim (x',y') \Rightarrow y = y' \Rightarrow y' = y \Rightarrow (x',y') \sim (x,y)$

c) Transitividad.

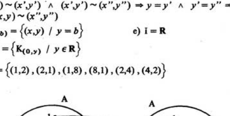
$(x,y) \sim (x',y') \;\wedge\; (x',y') \sim (x'',y'') \Rightarrow y = y' \;\wedge\; y' = y'' \Rightarrow y = y'' \Rightarrow$
$\Rightarrow (x,y) \sim (x'',y'')$

d) $K_{(a,b)} = \left\{(x,y) \;/\; y = b\right\}$ e) $I = \mathbf{R}$

f) $\dfrac{\mathbf{R}^2}{\sim} = \left\{K_{(0,y)} \;/\; y \in \mathbf{R}\right\}$

*3-24.* i ) $R = \left\{(1,2), (2,1), (1,8), (8,1), (2,4), (4,2)\right\}$

ii )




iii) $R$ es a-reflexiva, simétrica, a-transitiva y no antisimétrica.

*3-25.* a) Reflexividad.

$(a,b) \in \mathbf{N}^2 \Rightarrow a + b = b + a \Rightarrow (a,b) \sim (a,b)$

b) Simetría.
$(a,b) \sim (a',b') \Rightarrow a + b' = b + a' \Rightarrow a' + b = b' + a \Rightarrow (a',b') \sim (a,b)$

c) Transitividad.
$(a,b) \sim (a',b') \ \wedge \ (a',b') \sim (a'',b'') \Rightarrow a + b' = b + a' \wedge a' + b'' =$
$= b' + a'' \Rightarrow a + b' + a' + b'' = b + a' + b' + a'' \Rightarrow a + b'' = b + a'' \Rightarrow$
$\Rightarrow (a,b) \sim (a'',b'')$

d) Clases de equivalencia.
$K_{(a,b)} = \left\{(x,y) \in \mathbf{N}^2 \ / \ x + b = y + a\right\}$

e) Conjunto de índices. $I = \left\{(n, 1)\right\} \cup \left\{(1, n+1)\right\}$ con $n \in \mathbf{N}$
Ver 9.10

**3-26.** $R = \left\{(a,a), (b,b), (c,c), (d,d), (b,c), (c,b)\right\}$

**3-27.** a) $R = \left\{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1)\right\}$

b) Reflexividad.
$x \in A \Rightarrow x = x \Rightarrow (x,x) \in R$

c) Simetría.
$(x,y) \in R \Rightarrow x = y \ \vee \ x + y = 3 \Rightarrow y = x \ \vee \ y + x = 3 \Rightarrow (y,x) \in R$

d) Transitividad.
$(x,y) \in R \ \wedge \ (y,z) \in R \Rightarrow (x = y \ \vee \ x + y = 3) \ \wedge \ (y = z \ \vee \ z + y =$
$= 3) \Rightarrow x = z \ \vee \ x + z = 3 \Rightarrow (x,z) \in R$

e) La partición de A es $\dfrac{A^2}{\sim} = \left\{\left\{1, 2\right\}, \left\{3\right\}, \left\{4\right\}\right\}$

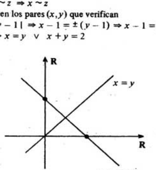
**3-28.** $R$ es de equivalencia.

**3-29.** i ) $x \in \mathbf{R} \Rightarrow |x - 1| = |x - 1| \Rightarrow x \sim x$

ii ) $x \sim y \Rightarrow |x - 1| = |y - 1| \Rightarrow |y - 1| = |x - 1| \Rightarrow y \sim x$

iii) $x \sim y \ \wedge \ y \sim z \Rightarrow x \sim z$

iv) A $R$ pertenecen los pares $(x, y)$ que verifican
$|x - 1| = |y - 1| \Rightarrow x - 1 = \pm (y - 1) \Rightarrow x - 1 = y - 1 \ \vee \ x - 1 =$
$= -y + 1 \Rightarrow x = y \ \vee \ x + y = 2$



**3-30.** i ) Simetría.

$(a,b) \in R \Rightarrow (a,b) \in R \ \wedge \ (b,b) \in R \Rightarrow (b,a) \in R$

Transitividad.

$(a,b) \in R \ \wedge \ (b,c) \in R \Rightarrow (c,a) \in R \Rightarrow (a,c) \in R$

ii ) Si $R$ es de equivalencia, entonces es reflexiva y circular, pues

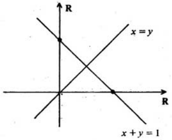
$(a,b) \in R \ \wedge \ (b,c) \in R \Rightarrow (a,c) \in R \Rightarrow (c,a) \in R$

**3-31.** i ) $R$ es de equivalencia. Se prueba siguiendo los esquemas anteriores.

ii ) $(x,y) \in R \Leftrightarrow x^2 - x = y^2 - y \Leftrightarrow x^2 - y^2 = x - y \Leftrightarrow$

$\Leftrightarrow (x+y)(x-y) - (x-y) = 0 \Leftrightarrow (x-y)(x+y-1) = 0 \Leftrightarrow$

$\Leftrightarrow x = y \ \vee \ x + y = 1$




iii) $K_a = \{x \in \mathbf{R} \ / \ x \sim a\}$

$x \sim a \Rightarrow x^2 - x = a^2 - a \Rightarrow x = a \ \vee \ x = 1 - a$

O sea $K_a = \{a, 1-a\}$

iv) $I = \left[\frac{1}{2}, \infty\right)$

v ) $\frac{\mathbf{R}}{\sim} = \left\{K_u \ / \ u \in \left[\frac{1}{2}, \infty\right)\right\}$

**3-32.** i ) $x \in A \Rightarrow (x,x) \in R \Rightarrow (x,x) \in R \cup S$

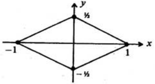
ii ) $x \in A \Rightarrow (x,x) \in R \ \wedge \ (x,x) \in S \Rightarrow (x,x) \in R \cap S$

**3-33.** $|x| + 2|y| = 1 \Rightarrow \pm x \pm 2y = 1 \Rightarrow x + 2y = 1 \ \vee \ x - 2y = 1 \ \vee$

$\vee \ -x + 2y = 1 \ \vee \ -x - 2y = 1 \Rightarrow$

$\Rightarrow \frac{x}{1} + \frac{y}{½} = 1 \ \vee \ x + \frac{y}{-½} = 1 \ \vee \ \frac{x}{-1} + \frac{y}{½} = 1 \ \vee \ \frac{x}{-1} + \frac{y}{-½} = 1$

con $|x| \leqslant 1 \ \wedge \ |y| \leqslant \frac{1}{2}$

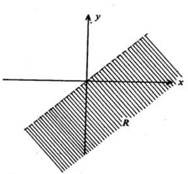



$D_R = [-1, 1]$

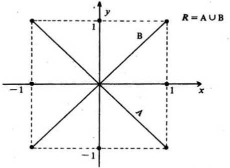
$I_R = \left[-\frac{1}{2}, \frac{1}{2}\right]$

*3-34.* $(a,b) \in R \cup R^{-1} \Rightarrow (a,b) \in R \ \vee \ (a,b) \in R^{-1} \Rightarrow (b,a) \in R^{-1} \ \vee \ (b,a) \in R \Rightarrow$
$\Rightarrow (b,a) \in R^{-1} \cup R \Rightarrow (b,a) \in R \cup R^{-1}$

*3-35.* i ) $R$ es a-reflexiva, a-simétrica, transitiva y antisimétrica.
ii ) $(x,y) \in R \Leftrightarrow x - y \in \mathbf{R}^+ \Leftrightarrow x - y > 0$




*3-36.* i ) $(x,y) \in R \Leftrightarrow x^2 = y^2 \Leftrightarrow x^2 - y^2 = 0 \Leftrightarrow (x+y)(x-y) = 0 \Leftrightarrow$
$\Leftrightarrow x + y = 0 \ \vee \ x - y = 0$ con $|x| \leqslant 1 \ \wedge \ |y| \leqslant 1$




ii ) $R$ es de equivalencia, pues:

a) $x \in A \Rightarrow x^2 = x^2 \Rightarrow x \sim x$

b) $x \sim y \Rightarrow x^2 = y^2 \Rightarrow y^2 = x^2 \Rightarrow y \sim x$

c) $x \sim y \ \wedge \ y \sim z \Rightarrow x^2 = y^2 \ \wedge \ y^2 = z^2 \Rightarrow x^2 = z^2 \Rightarrow x \sim z$

iii) $K_a = \left\{x \in A \,/\, x^2 = a^2\right\} = \left\{-a\,,\,a\right\}$

$\frac{A}{\sim} = \left\{K_u \,/\, u \in [0\,,1]\right\}$

***3-37.*** i ) $(a,b) \in R^{-1} \Rightarrow (b,a) \in R \Rightarrow (a,b) \in R \Rightarrow (b,a) \in R^{-1}$

ii ) $(a,b) \in R^{-1} \ \wedge \ (b,c) \in R^{-1} \Rightarrow (b,a) \in R \ \wedge \ (c,b) \in R \Rightarrow (c,b) \in R \Rightarrow$
$\Rightarrow (b,c) \in R^{-1}$

***3-38.*** $(a,b) \in R \cap R' \ \wedge \ (b,c) \in R \cap R' \Rightarrow$
$\Rightarrow (a,b) \in R \ \wedge \ (b,c) \in R \ \wedge \ (a,b) \in R' \ \wedge \ (b,c) \in R' \Rightarrow$
$\Rightarrow (a,c) \in R \ \wedge \ (a,c) \in R' \Rightarrow (a,c) \in R \cap R'$

***3-39.*** $(a,b) \in R \cap R' \ \wedge \ (b,a) \in R \cap R' \Rightarrow$
$\Rightarrow (a,b) \in R \ \wedge \ (b,a) \in R \ \wedge \ (a,b) \in R' \ \wedge \ (b,a) \in R' \Rightarrow a = b$

***3-40.*** i ) $a \in X \Rightarrow a \in A \Rightarrow a \sim a \Rightarrow a \in X^*$

ii ) $a \in (X \cup Y)^* \Leftrightarrow a \sim b\,,\ \forall b \in X \cup Y \Rightarrow$
$\Leftrightarrow (a \sim b\,,\ \forall b \in X) \ \vee \ (a \sim b\,,\ \forall b \in Y) \Leftrightarrow$
$\Leftrightarrow a \in X^* \ \vee \ a \in Y^* \Leftrightarrow a \in X^* \cup Y^*$

***3-41.*** i ) $R$ es reflexiva, simétrica, no transitiva y no antisimétrica.

ii ) $R$ es a-reflexiva, simétrica, a-transitiva y no antisimétrica.

*3-42.*

| | $R_1$ | $R_2$ | $R_3$ | $R_4$ | $R_5$ | $R_6$ | $R_7$ | $R_8$ | $R_9$ | $R_{10}$ | $R_{11}$ | $R_{12}$ | $R_{13}$ | $R_{14}$ | $R_{15}$ | $R_{16}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R | no | no | no | no | no | no | no | sí | no | no | no | no | sí | sí | no | sí |
| S | sí | sí | no | no | sí | no | no | sí | sí | no | no | sí | no | no | sí | sí |
| T | sí | sí | sí | sí | sí | sí | sí | sí | no | sí | sí | no | sí | sí | no | sí |
| A | sí | sí | sí | sí | sí | sí | sí | sí | no | sí | sí | no | sí | sí | no | no |

*3-43.* $R$ es no reflexiva, simétrica, no transitiva y no antisimétrica.

*3-44.* $R = \{(1,1), (1,2), (1,3), (1,4), (1,5), (2,2), (2,3), (2,4), (2,5), (3,3), (3,4), (3,5), (4,4), (4,5), (5,5)\}$

Elementos minimales: 1
Elementos maximales: 5

*3-45.* $R = \{(1,1), (1,2), (1,3), (1,4), (1,5), (2,2), (2,4), (3,3), (4,4), (5,5)\}$

Elemento minimal: 1
Elementos maximales: 4, 5 y 6

*3-46.* Cota inferior: 1. Cota superior: 6.

*3-47.* i ) A no tiene primer elemento, pero el último es 1.

ii ) No está bien ordenado pues el mismo A carece de primer elemento.

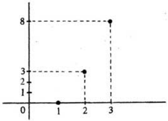
iii) Cotas inferiores son todos los reales no positivos. Cotas superiores son los reales mayores o iguales que 1.

iv) El ínfimo o extremo inferior es $0 \notin A$. El supremo o extremo superior es $1 \in A$.

## TRABAJO PRACTICO IV

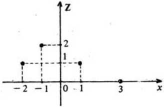
*4-25.* i ) $f = \{(1,0), (2,3), (3,8)\}$

ii )



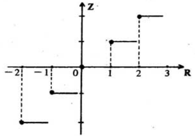

iii) $f$ es inyectiva, no sobreyectiva ni biyectiva.

*4-26.* i )



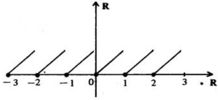

ii ) $f$ es no inyectiva, no sobreyectiva, no biyectiva.

*4-27.* i )



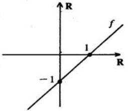

ii ) $f$ no es inyectiva, es sobreyectiva y no biyectiva.

*4-28.* i )



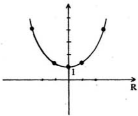

ii ) no es inyectiva, ni sobreyectiva, ni biyectiva.

*4-29.* i )



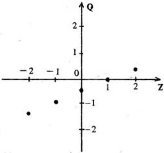

biyectiva.

ii)




no inyectiva, sobreyectiva, no biyectiva.

iii)




*f* es inyectiva, no sobreyectiva, no biyectiva.

***4-30.*** Representando *f* por una tabla

| $(a,b)$ | $(1,1)$ | $(1,2)$ | $(1,3)$ | $(2,1)$ | $(2,2)$ | $(2,3)$ |
|---|---|---|---|---|---|---|
| $f(a,b)$ | 2 | 1 | 0 | 5 | 4 | 3 |

Puede hacerse un gráfico en tres dimensiones. *f* es inyectiva, no sobreyectiva, ni biyectiva.

4-31.

| X | $\phi$ | $\{1\}$ | $\{2\}$ | $\{3\}$ | $\{1,2\}$ | $\{1,3\}$ | $\{2,3\}$ | A |
|---|---|---|---|---|---|---|---|---|
| $f(X)$ | B | $\{2,3,4\}$ | $\{1,3,4\}$ | $\{1,2,4\}$ | $\{3,4\}$ | $\{2,4\}$ | $\{1,3\}$ | $\{4\}$ |

$f$ es inyectiva, no sobreyectiva, no biyectiva.

4-32. Se presentan infinitas posibilidades.

4-33. $f(A)=\{1,4,9,16\}$ $\quad f(B)=\{1,4,9,16\}$

$f(A\cap B)=\{4\}$ $\quad f(A\cup B)=\{1,4,9,16\}$

Resulta $f(A\cup B)=f(A)\cup f(B)$ y $f(A\cap B)\subset f(A)\cap f(B)$

4-34. Verificar tomando $A=\{(1,2),(2,2),(3,3)\}$ y $B=\{(1,2)\}$

4-35. i ) Considerar $X=\{1,2,3\}$, $Y=\{1,2,3,4\}$, $f: X\rightarrow Y$ definida por $f(x)=x$ y $A=\{1,2\}\subset X$.

ii ) Tomar, por ejemplo, $X=\{1,2,3\}$, $Y=\{1,2\}$, $f: X\rightarrow Y$ tal que $f(1)=1$, $f(2)=2$, $f(3)=2$, y $A=\{1,2\}$

iii) Proponer una situación del tipo anterior.

4-36. $f^{-1}[-1,1)=\phi \quad f^{-1}\left(-\infty,\frac{1}{2}\right]=\phi \quad f^{-1}[0,3]=[-\sqrt{2},\sqrt{2}]$

$f^{-1}[0,3)=[-\sqrt{2},\sqrt{2})\qquad f^{-1}[1,10]=[-3,3]$

4-37. i ) $x\in A\Rightarrow f(x)\in f(A)\Rightarrow x\in f^{-1}[f(A)]$

O sea $A\subset f^{-1}[f(A)]$ (1)

Suponemos que existe $y\in f^{-1}[f(A)]\wedge y\notin A$ pero como existe $x\in A/f(x)=f(y)$, resulta $f$ no inyectiva, lo que es absurdo. Luego

$$f^{-1}[f(A)]\subset A \qquad (2)$$

De (1) y (2) resulta la igualdad.

ii ) Si existen $x\neq y$ tales que $f(x)=f(y)$, entonces considerando $A=\{x\}$ se tiene

$A=\{x\}\neq\{x,y\}\subset f^{-1}[f(A)]$

4-38. i ) $g\circ f: Z\rightarrow Z\,/\,(g\circ f)(x)=\text{ent}\left(\frac{x^2}{2}+1\right)$

ii ) $f\circ g: Q\rightarrow Q\,/\,(f\circ g)(x)=\frac{[\text{ent}(x)]^2}{2}+1$

iii) $(g\circ f)(-2)=3$ y $(f\circ g)\left(-\frac{1}{2}\right)=\frac{3}{2}$

4-39. Como por hipótesis: $\forall z\in C,\exists x\in A\,/\,(g\circ f)(x)=g[f(x)]=z\Rightarrow$ $\Rightarrow \forall z\in C,\exists y=f(x)\in B\,/\,g(y)=z$ resulta $g$ sobreyectiva.

**4-40.** $g \circ f$ es biyectiva $\Rightarrow f$ es inyectiva $\wedge$ $g$ es sobreyectiva.
$h \circ g$ es biyectiva $\Rightarrow g$ es inyectiva $\wedge$ $h$ es sobreyectiva.
Luego, $g$ es biyectiva y en consecuencia $g^{-1}$ es biyectiva. Entonces $g^{-1} \circ (g \circ f) = (g^{-1} \circ g) \circ f = i_B \circ f = f$ es biyectiva y $(h \circ g) \circ g^{-1} = h \circ i_C = h$ es biyectiva.

**4-41.** Como $h \circ g \circ f = (h \circ g) \circ f = h \circ (g \circ f)$ es sobreyectiva resultan $h \circ g$ y $h$, sobreyectivas por 4-39. Análogamente
$f \circ h \circ g$ sobreyectiva $\Rightarrow f \circ h$ y $f$ sobreyectivas.
$g \circ f \circ h$ inyectiva $\Rightarrow h$ y $f \circ h$ inyectivas.
Resulta $f \circ h$ biyectiva y $h$ biyectiva.
Luego $(f \circ h) \circ h^{-1} = f$ es biyectiva.
Como $h \circ g$ y $h^{-1}$ son sobreyectivas, es $h^{-1} \circ (h \circ g) = g$ sobreyectiva. Por otra parte, como $g \circ (f \circ h)$ y $(f \circ h)^{-1}$ son inyectivas, su composición $g$ también lo es.
Luego $g$ es también biyectiva.

**4-42** a) $x \in A \Rightarrow f(x) \in f(A) \Rightarrow x \in f^{-1}[f(A)]$
O sea $A \subset f^{-1}[f(A)]$

b) $y \in f[f^{-1}(B)] \Rightarrow \exists\, x \in f^{-1}(B) \,/\, y = f(x) \in f[f^{-1}(B)] \Rightarrow$
$\Rightarrow y = f(x) \in B.$

c) $f(X) - f(A) = f(X) \cap [f(A)]^c \subset f(X) \cap f(A^c) \subset f(X \cap A^c) = f(X - A)$

d) $f^{-1}(Y - B) = f^{-1}(Y \cap B^c) = f^{-1}(Y) \cap f^{-1}(B^c) =$
$= X \cap [f^{-1}(B)]^c = X - f^{-1}(B)$

e) $f(A \cap f^{-1}(B)) \subset f(A) \cap f[f^{-1}(B)] \subset f(A) \cap B$ por b)
Además
$y \in f(A) \cap B \Rightarrow y \in f(A) \;\wedge\; y \in B \Rightarrow$
$\Rightarrow \exists\, x \in A \,/\, y = f(x) \in A \;\wedge\; f(x) \in B \Rightarrow$
$\Rightarrow x \in A \;\wedge\; x \in f^{-1}(B) \Rightarrow x \in A \cap f^{-1}(B) \Rightarrow$
$\Rightarrow f(x) \in f(A \cap f^{-1}(B))$

**4-43.** i ) Sea $x \in A \cap B \Rightarrow x \in A \;\wedge\; x \in B$. Luego
$\chi_{A \cap B}(x) = 1 \;\wedge\; \chi_A(x) = 1 \;\wedge\; \chi_B(x) = 1$ , o sea
$\chi_{A \cap B}(x) = \chi_A(x)\, \chi_B(x)$
Análogamente se analiza el caso $x \notin A \cap B$

ii ) Para la función característica de la unión se procede en forma similar.

**4-44.** $(f \circ d)(a) = f[d(a)] = f(a,a) = (a,a) = d(a)$
Luego $f \circ d = d$

**4-45.** i ) $f(x + y) = (x + y, -x - y) = (x, -x) + (y, -y) = f(x) + f(y)$
ii ) $f(kx) = (kx, -kx) = k(x, -x) = k f(x)$

**4-46.** i ) $w \in \bigcap\limits_{n=1}^{\infty} f^{-1}(-\infty, x + 2^{-n}) \Rightarrow w \in f^{-1}(-\infty, x + 2^{-n}),\ \forall n \Rightarrow$

$\Rightarrow \forall n : f(w) \in (-\infty, x + 2^{-n}) \Rightarrow \forall n : f(w) < x + 2^{-n}$ (1)
Resulta $f(w) \leqslant x$ ya que si fuera $f(w) > x \Rightarrow$
$\Rightarrow f(w) - x > 0 \Rightarrow \exists\, n_0 \in N / f(w) - x \geqslant 2^{-n_0} \Rightarrow$
$\Rightarrow \exists\, n_0 / f(w) \geqslant x + 2^{-n_0}$, contradictorio con (1).
Entonces $f(w) \in (-\infty, x] \Rightarrow w \in f^{-1}(-\infty, x]$

ii) $w \in f^{-1}(-\infty, x] \Rightarrow f(w) \leqslant x$ y como $\forall n \in N : 0 < 2^{-n}$, se tiene $f(w) < x + 2^{-n}, \forall n$. Luego
$f(w) \in (-\infty, x + 2^{-n}) \Rightarrow w \in f^{-1}(-\infty, x + 2^{-n}), \forall n \Rightarrow$

$\Rightarrow w \in \bigcap_{n=1}^{\infty} f^{-1}(-\infty, x + 2^{-n})$

*4-47.* a) $\Omega + \phi = \Omega \Rightarrow P(\Omega) + P(\phi) = P(\Omega) \Rightarrow P(\phi) = 0$

b) $A \cup B = A + A^c B \Rightarrow P(A \cup B) = P(A) + P(A^c B)$ (1)
$B = AB + A^c B \Rightarrow P(AB) + P(A^c B) = P(B)$ (2)
Sumando (1) y (2)
$P(A \cup B) + P(AB) + \cancel{P(A^c B)} = P(A) + \cancel{P(A^c B)} + P(B) \Rightarrow P(A \cup B) =$
$= P(A) + P(B) - P(AB)$

c) $A + A^c = \Omega \Rightarrow P(A) + P(A^c) = P(\Omega) \Rightarrow P(A^c) = 1 - P(A)$

*4-48.* a) $\forall x \in R : X^{-1}(-\infty, x) \in A \Rightarrow X^{-1}(-\infty, x + 2^{-n}) \in A \Rightarrow$

$\Rightarrow \bigcap_{n=1}^{\infty} X^{-1}(-\infty, x + 2^{-n}) = X^{-1}(-\infty, x] \in A$, por 4-46

b) $\forall x \in R : X^{-1}(-\infty, x] \in A \Rightarrow X^{-1}(-\infty, x - 2^{-n}] \in A \Rightarrow$

$\Rightarrow \bigcap_{n=1}^{\infty} X^{-1}(-\infty, x - 2^{-n}] = X^{-1}(-\infty, x) \in A$, por 4-24.

*4-49.* $X^{-1}(-\infty, x] \in A \Leftrightarrow X^{-1}(-\infty, x) \in A$ (por 4-48) $\Leftrightarrow$
$\Leftrightarrow [X^{-1}(-\infty, x)]^c \in A$ (por 2-72) $\Leftrightarrow X^{-1}(-\infty, x)^c \in A$ por 4.9.2 c) $\Leftrightarrow$
$\Leftrightarrow X^{-1}[x, \infty) \in A$

*4-50.* $X^{-1}(-\infty, x] \in A \Leftrightarrow (X^{-1}(-\infty, x])^c \in A \Leftrightarrow X^{-1}(-\infty, x]^c \in A \Leftrightarrow$
$\Leftrightarrow X^{-1}(x, \infty) \in A$

*4-51.* i) $\Rightarrow$ ii) La condición i) equivale a la inyectividad de $f$, por 4-37. Entonces
$f(x) \in f(A \cap B) \Leftrightarrow x \in f^{-1}[f(A \cap B)] \Leftrightarrow x \in A \cap B \Leftrightarrow$
$\Leftrightarrow x \in A \ \wedge \ x \in B \Leftrightarrow f(x) \in f(A) \ \wedge \ f(x) \in f(B) \Leftrightarrow f(x) \in A \cap B.$

ii) $\Rightarrow$ iii) $f(A) \cap f(B) = f(A \cap B) = f(\phi) = \phi$

iii) $\Rightarrow$ iv) $(A - B) \cap B = \phi \Rightarrow f(A - B) \cap f(B) = \phi$ (1)
$(A - B) \cup B = A \Rightarrow f(A - B) \cup f(B) = f(A)$ (2)
De (1) y (2), por 2-65, resulta $f(A - B) = f(A - B) = f(A) - f(B)$

iv) $\Rightarrow$ i) Suponemos $f^{-1}[f(A)] \neq A \Rightarrow \exists\, x \notin A \ \wedge \ f(x) \in f(A)$
Sea $M = A \cup \{x\} \Rightarrow A \subset M \Rightarrow$
$\Rightarrow f(M - A) = f(M) - f(A) \Rightarrow f(\{x\}) = \phi \Rightarrow$
$\Rightarrow f$ no es función.

## TRABAJO PRACTICO V

*5-21.* i ) Conmutatividad.

$a * b = 2(a+b) = 2(b+a) = b * a$

ii ) $*$ no es asociativa, pues

$(3 * 2) * (-2) = 10 * (-2) = 16$

$3 * [2 * (-2)] = 3 * 0 = 8$

iii) No existe neutro $e$ ya que

$a * e = a \Rightarrow 2(a+e) = a \Rightarrow 2a + 2e = a \Rightarrow e = -\dfrac{a}{2}$.

iv) Los elementos de $\mathbf{Z}$ no admiten inverso porque no existe neutro;

v ) Regularidad.

$a * b = a * c \Rightarrow 2(a+b) = 2(a+c) \Rightarrow a + b = a + c \Rightarrow b = c$

O sea, todos los enteros son regulares respecto de $*$.

*5-22.* Está demostrado en 5.3.5.

*5-23.* Siendo $f_1 = \{(1,1),(2,2),(3,3)\}$, $f_2 = \{(1,1),(2,3),(3,2)\}$,
$f_3 = \{(1,2),(2,1),(3,3)\}$, $f_4 = \{(1,2),(2,3),(3,1)\}$,
$f_5 = \{(1,3),(2,1),(3,2)\}$, $f_6 = \{(1,3),(2,2),(3,1)\}$, resulta

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
|---|---|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
| $f_2$ | $f_2$ | $f_1$ | $f_4$ | $f_3$ | $f_6$ | $f_5$ |
| $f_3$ | $f_3$ | $f_5$ | $f_1$ | $f_6$ | $f_2$ | $f_4$ |
| $f_4$ | $f_4$ | $f_6$ | $f_2$ | $f_5$ | $f_1$ | $f_3$ |
| $f_5$ | $f_5$ | $f_3$ | $f_6$ | $f_1$ | $f_4$ | $f_2$ |
| $f_6$ | $f_6$ | $f_4$ | $f_5$ | $f_2$ | $f_3$ | $f_1$ |

*5-24.* $a * a' = a' * a = e \Rightarrow a$ es inverso de $a' \Rightarrow a = (a')'$

*5-25.* $(b' * a') * (a * b) = b' * (a' * a) * b = b' * e * b = b' * b = e = (a * b) * (b' * a')$
$= (a * b) * (b' * a') \Rightarrow (a * b)' = b' * a'$

*5-26.* $*$ es conmutativa, asociativa, con neutro $e = -4$, con inverso $a' = -a - 8$ para todo $a \in \mathbf{Z}$. Además, todos los elementos son regulares. Seguir el procedimiento del ejemplo 5-6.

*5-27.* $a \sim b \ \wedge \ c \sim d \Rightarrow 2|a - b \ \wedge \ 2|c - d \Rightarrow 2|(a-b) + (c-d) \Rightarrow$
$\Rightarrow 2|(a+c) - (b+d) \Rightarrow 2|(a+c+4) - (b+d+4) \Rightarrow$
$\Rightarrow 2|(a * c) - (b * d) \Rightarrow a * c \sim b * d.$

*5-28.* $*$ es asociativa, conmutativa, no existen neutro ni inversos, y ningún real es regular.

*5-29.* $\perp$ no es asociativa no conmutativa; no existen neutro ni inversos; sin embargo, todos los elementos de $\mathbf{Q}^*$ son regulares.

*5-30.* Por definición $a * b = \text{mín}\{a,b\}$. Esta ley interna es conmutativa y asociativa. No existen neutro ni inversos, y ningún elemento es regular.

*5-31.* La suma de funciones en $\mathbf{R}^{\mathbf{I}}$ es conmutativa, asociativa, con neutro $e: \mathbf{I} \rightarrow \mathbf{R}$ definida por $e(x) = 0$, $\forall x \in \mathbf{I}$, y el inverso aditivo de todo elemento $f \in \mathbf{R}^{\mathbf{I}}$ es $-f: \mathbf{I} \rightarrow \mathbf{R}$, tal que $(-f)(x) = -f(x)$. Además, todos los elementos son regulares. Demostramos la conmutatividad

$(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x) \Rightarrow f + g = g + f.$

*5-32.* $f_1 = \{(a,a), (b,b)\}$, $f_2 = \{(a,a), (b,a)\}$, $f_3 = \{(a,b), (b,b)\}$,
$f_4 = \{(a,b), (b,a)\}$

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
| $f_2$ | $f_2$ | $f_2$ | $f_3$ | $f_4$ |
| $f_3$ | $f_3$ | $f_2$ | $f_3$ | $f_2$ |
| $f_4$ | $f_4$ | $f_2$ | $f_3$ | $f_1$ |

*5-33.* $f$ no es conmutativa, pues $f(1,3) = 10 \neq f(3,1) = 4$;
$f$ no es asociativa ya que $f[f(a,b), c] = f(a,b) + c^2 = a + b^2 + c^2$ y
$f[a, f(b,c)] = f(a, b + c^2) = a + (b + c^2)^2$.
No existe neutro, pues $f(a, e) = a \Rightarrow a + e^2 = a \Rightarrow e = 0$ y
$f(e, a) = a \Rightarrow e + a^2 = a \Rightarrow e = a - a^2$

Sólo existe neutro a derecha, y es 0. Todos los elementos son regulares a derecha, pero no a izquierda.

*5-34.* i ) Asociatividad.

$(a * b) * c = (a * b) * (e * c) = (a * e) * (b * c) = a * (b * c).$

ii ) Conmutatividad.

$a * b = (e * a) * (b * e) = (e * b) * (a * e) = b * a.$

**5-35.** Seguir el procedimiento indicado en 5-26. El neutro es $e = \frac{1}{3}$ y el inverso de todo elemento $a$, es $a' = \frac{1}{9a}$

**5-36.** Demostramos la asociatividad
$[f(gh)](x) = f(x)(gh)(x) = f(x)[g(x)h(x)] = [f(x)g(x)]h(x) =$
$= (fg)(x)h(x) = [(fg)h](x) \Rightarrow f(gh) = (fg)h.$

**5-37.** i ) $a * (b * z) = a * (bz) = a(bz) = (ab)z = (ab) * z.$
Análogamente se prueban ii ) y iii).

**5-38.** i ) $f$ es un morfismo, pues
$f(ab) = \log_2(ab) = \log_2 a + \log_2 b = f(a) + f(b)$

ii ) $f$ es $1-1$, pues si $x'$ y $x''$ son reales positivos que verifican $f(x') = f(x'')$, entonces $\log_2 x' = \log_2 x'' = y \Rightarrow x' = x'' = 2^y$

iii) $f$ es sobreyectiva, pues
$\forall y \in \mathbf{R}, \exists x = 2^y / f(x) = \log_2 x = \log_2 2^y = y$

**5-39.** $f(xy) = sg(xy) = sg\, x \,.\, sg\, y = f(x) f(y)$ considerando todas las alternativas.

**5-40.** $(x \circ y) * x = (x + y) * z = x + y = (x * z) + (y * z) = (x * z) \circ (y * z)$
$z * (x \circ y) = z * (x + y) = z \neq (z * x) \circ (z * y) = z \circ z = z + z = 2z.$
Entonces $*$ es distributiva a derecha respecto de $\circ$, pero no lo es a izquierda.

## TRABAJO PRACTICO VI

*6-36.* Demostramos los siguientes casos

2. i ) $n = 1 \Rightarrow \sum_{i=1}^{1} \frac{i}{2^i} = \frac{1}{2} = 2 - \frac{3}{2} = 2 - \frac{1+2}{2^i}$

ii ) $\sum_{i=1}^{h} \frac{i}{2^i} = 2 - \frac{h+2}{2^h} \Rightarrow \sum_{i=1}^{h+1} \frac{i}{2^i} = 2 - \frac{h+3}{2^{h+1}}$

D) $\sum_{i=1}^{h+1} \frac{i}{2^i} = \sum_{i=1}^{h} \frac{i}{2^i} + \frac{h+1}{2^{h+1}} = 2 - \frac{h+2}{2^h} + \frac{h+1}{2^{h+1}} =$

$= 2 - \frac{2(h+2)-(h+1)}{2^{h+1}} = 2 - \frac{h+3}{2^{h+1}}$

8. i ) $n = 1 \Rightarrow (1+x)^1 = 1 + x = 1 + 1 \,.\, x \geqslant 1 + 1 \,.\, x$

ii ) $(1+x)^h \geqslant 1 + hx \Rightarrow (1+x)^{h+1} \geqslant 1 + (h+1)x$

D) $(1+x)^{h+1} = (1+x)^h (1+x) \geqslant (1+hx)(1+x) =$

$= 1 + x + hx + hx^2 = 1 + (h+1)x + hx^2 > 1 + (h+1)x$

11. i ) $n = 1 \Rightarrow 2 | 1^2 + 1$

ii ) $h^2 + h = 2k \Rightarrow (h+1)^2 + (h+1) = 2k'$

D) $(h+1)^2 + (h+1) = h^2 + 2h + 1 + h + 1 = (h^2 + h) + 2(h+1) =$

$= 2k + 2(h+1) = 2(k+h+1) = 2k'$

15. i ) $n = 1 \Rightarrow \sum_{i=1}^{1} i^3 = 1^3 = 1^2 = \left(\sum_{i=1}^{1} i\right)^2$

ii ) $\sum_{i=1}^{h} i^3 = \left(\sum_{i=1}^{h} i\right)^2 \Rightarrow \sum_{i=1}^{h+1} i^3 = \left(\sum_{i=1}^{h+1} i\right)^2$

D) $\sum_{i=1}^{h+1} i^3 = \sum_{i=1}^{h} i^3 + (h+1)^3 = \left(\sum_{i=1}^{h} i\right)^2 + (h+1)^3 =$

$= \frac{h^2 (h+1)^2}{4} + (h+1)^3 = (h+1)^2 \left[\frac{h^2}{4} + (h+1)\right] =$

$= (h+1)^2 \frac{h^2 + 4h + 4}{4} = \frac{(h+1)^2 (h+2)^2}{4} = \left[\frac{(h+1)(h+2)}{2}\right]^2 =$

$= \left(\sum_{i=1}^{h+1} i\right)^2$ . Se ha tenido en cuenta el resultado del ejemplo 6-3.

*6-37.* $\sum_{i=1}^{n} (x_i - \bar{x}) = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} \bar{x} = n\,\bar{x} - n\,\bar{x} = 0$

*6-38.* i ) $n = 2 \Rightarrow \left(\sum_{i=1}^{2} x_i\right)^2 = (x_1 + x_2)^2 = x_1^2 + x_2^2 + 2\,x_1\,x_2 =$

$= \sum_{i=1}^{2} x_i^2 + \sum_{i \neq j}^{2} x_i\,x_j$

ii ) $\left(\sum_{i=1}^{h} x_i\right)^2 = \sum_{i=1}^{h} x_i^2 + \sum_{i \neq j}^{h} x_i\,x_j \Rightarrow \left(\sum_{i=1}^{h+1} x_i\right)^2 = \sum_{i=1}^{h+1} x_i^2 + \sum_{i \neq j}^{h+1} x_i\,x_j$

D) $\left(\sum_{i=1}^{h+1} x_i\right)^2 = \left(\sum_{i=1}^{h} x_i + x_{h+1}\right)^2 = \left(\sum_{i=1}^{h} x_i\right)^2 + 2\,x_{h+1} \sum_{i=1}^{h} x_i + x_{h+1}^2 =$

$= \sum_{i=1}^{h} x_i^2 + \sum_{i \neq j}^{h} x_i\,x_j + \sum_{i=1}^{h} x_i\,x_{h+1} + \sum_{i=1}^{h} x_{h+1}\,x_i + x_{h+1}^2 =$

$= \sum_{i=1}^{h+1} x_i^2 + \sum_{i \neq j}^{h+1} x_i\,x_j$

*6-39.* $\sum_{i=1}^{10} (x_i - 2)^2 = \sum_{i=1}^{10} (x_i^2 - 4\,x_i + 4) = \sum_{i=1}^{10} x_i^2 - 4 \sum_{i=1}^{10} x_i + \sum_{i=1}^{10} 4 =$
$= 100 - 4 \,.\, 10\,\bar{x} + 40 = 140 - 40\,(-20) = 140 + 800 = 940$

*6-40.* Utilizar la definición de la función factorial.

*6-41.* Considerar las dos posibilidades
$x^2 - x = 2\,x - 2 \;\vee\; x^2 - x + 2\,x - 2 = 7$
Resulta $x = 2 \;\vee\; x = 1$

*6-42.* i ) $64\,a^{12} - 192\,a^9 + 240\,a^2 - 160 + 80\,a^{-2} - 12\,a^{-4} + a^{-6}$
ii ) $x^2 + y^2 + 6\,xy + 4\,(x + y)\,\sqrt{xy}$

*6-43.* i ) $\sum_{k=0}^{m} \binom{n}{k} p^{n-k}\,q^k = (p + q)^n = 1^n = 1$

ii ) $\left(\frac{2 + t}{3}\right)^n$

*6-44.* $T_5 + T_7 = 210\,(64\,x^{14} + 16\,x^{16})$

*6-45.* $x = \pm\,2 \;\vee\; x = \pm\,2\,i$

*6-46.* Soluciones reales son $x = 0 \;\vee\; x = \frac{3}{4}$

*6-47.* $T_6 = -\binom{10}{5} x^5$

*6-48.* Los términos de grado natural son los 5 primeros: $T_1, T_2, \ldots, T_5$.

*6-49.* 10! 3!

*6-50.* Con las dos personas juntas se tienen 9! 2! posibilidades. Con tales personas separadas, resultan $10! - 9!\,2! = (10-2)\,9! = 8\,.\,9!$ casos.

*6-51.* 66 . 660.

*6-52.* 5!

*6-53.* $C_{8,2} - C_{4,2} + 1 = 23$

*6-54.* Con $i$ varones y $6-i$ mujeres se pueden formar $C_{8,i}\cdot C_{9,6-i}$. El número total es $\sum_{i=0}^{6} C_{8,i}\,.\,C_{9,6-i}$.

*6-55.* Hay tantas distribuciones posibles como funciones crecientes de $I_{100}$ en $I_{10}$, o sea $C'_{100,10} = C_{109,10}$

*6-56.* $V_{6,3} - V_{5,2} = 6\,.\,5\,.\,4 - 5\,.\,4 = 125$. Los números cuya primera cifra (centenas) es 0, son $V_{5,2}$.

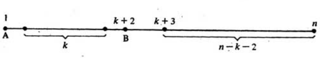
*6-57.* Como no se exige que las cifras sean distintas, resulta $V'_{6,3} - V'_{6,2} = 6^3 - 6^2 = 6^2\,.\,5 = 180$

*6-58.* $C_{4,2}\,.\,C_{48,3}$ es el número de muestras de tamaño 5 que contienen exactamente 2 ases.

*6-59.* $C_{4,2}\,.\,C_{32,1} = 6\,.\,32 = 192$

*6-60.* $P_k^{4,k-4}\,.\,V'_{8,k-4} = \dfrac{k!}{4!\,(k-4)!}\;8^{k-4} = \dbinom{k}{4}\,.\,8^{k-4}$

*6-61.* $(n-k-1)!\;k!\;2!$




*6-62.* No se piden restricciones en cuanto a convexidad, y pueden formarse $\dfrac{V_{10,3}}{2\,.\,3}$ triángulos, hasta $\dfrac{V_{10,10}}{2\,.\,10}$ decágonos. El número total es $\sum_{i=3}^{10} \dfrac{V_{10,i}}{2i}$ polígonos.

*6-63.* 2 . 5! 5!

*6-64.* i ) Tantas como funciones de $I_n$ en $I_3$, o sea $V'_{3,n} = 3^n$.

ii ) $P_n^{k,\,n-k}\;\;.\;\;V'_{2,\,n-k}$

**6-65.** i ) $V'_{3,13} = 3^{13}$

ii ) $P_{13}^{k,\,13-k} \quad V'_{2,13-k} = \dfrac{13!}{k!\,(13-k)!} \cdot 2^{13-k}$

**6-66.** Sean $A = \{x_1, x_2, \ldots, x_n, \ldots\}$ numerable y $M \subset A$, infinito.
Consideramos $x_{i_1}$ el primer elemento de A perteneciente a M, el cual existe por el principio de buena ordenación; de los que le siguen en A, elegimos el primero, $x_{i_2}$, perteneciente a M. Siempre es posible obtener uno porque M es infinito. Resulta

$M = \left\{ x_{i_1}, x_{i_2}, x_{i_3}, \ldots \right\}$ numerable.

**6-67.** Sean $A_i = \left\{ a_{i_1}, a_{i_2}, \ldots, a_{i_n}, \ldots \right\}$ con $i \in I_n$.
Consideramos la unión disjunta $\sum\limits_{i=1}^{n} A_i$ y la función

$$f : \sum_{i=1}^{n} A_i \to N$$

definida por $f(a_{ij}) = (j-1)\,n + i$ (según una ordenación por columnas). Como $f$ es biyectiva, resulta $\sum\limits_{i=0}^{n} A_i \sim N$.

**6-68.** i ) $V'_{4,12} = 4^{12}$ ii ) $P_{12}^{3,3,3,3} = \dfrac{12!}{3!\,3!\,3!\,3!}$

**6-69.** $C'_{5,5} = C_{9,5}$

**6-70.** i ) $C_{6,3} \cdot C_{8,4}$ ii ) $C_{5,2} \cdot C_{8,4}$ iii) $C_{6,3} \cdot C_{6,4}$

## TRABAJO PRACTICO VII

*7-10.* Se niega cada axioma del sistema dado. Como $A_1 : \forall a : a \in A \Rightarrow (a,a) \in R$, su negación es $\sim A_1 : \exists a / a \in A \wedge (a,a) \notin R$. El sistema $\sim A_1, A_2, A_3$ debe ser compatible, para lo cual es suficiente exhibir un modelo. La interpretación $A = \{1, 2, 3\}$, $R = \{(1,1), (2,2)\}$ es un modelo. Esto prueba la independencia de $A_1$. Análogamente se procede respecto de la independencia de $A_2$ y $A_3$.

*7-11.* I. $(a,b) \in R \Rightarrow a \neq b \Rightarrow (a,b) \in R \vee (b,a) \in R$ en virtud de $A_2$ y de $A_1$. Resulta $(b,a) \notin R$, porque en caso contrario, por $A_3$ y $A_2$

$(a,b) \in R \wedge (b,a) \in R \Rightarrow (a,a) \in R \Rightarrow a \neq a$

lo que es absurdo.

*7-12.* I. a) $1' = 0$. En efecto $1' = 1' \,.\, 1 = 1 \,.\, 1' = 0$

por $B_5$, $B_2$ y $B_6$.

b) $0' = 1$ por el principio de dualidad.

II. Suponemos que $a$ admite dos complementarios $a'$ y $a''$. Entonces.

$a' = a' + 0 = a' + (a.a'') = (a'+a) \,.\, (a'+a'') =$

$= (a+a') \,.\, (a'+a'') = 1 \,.\, (a'+a'') = (a'+a'') \,.\, 1 = a' + a''$.

Análogamente $a'' = a'' + a'$ y en consecuencia $a' = a''$.

III. $a + (a.b) = (a.1) + (a.b) = a.\,(1+b) = a \,.\, (b+1) = a \,.\, 1 = a$

Por dualidad resulta $a.\,(a+b) = a$.

*7-13.* Probamos que $n + b \neq n$

i) $n = 1 \Rightarrow 1 + b = b + 1 = s(b) \neq 1$

ii) $h + b \neq h \Rightarrow s(h) + b \neq s(h)$

D) $s(h) + b = b + s(h) = s(b+h) \neq s(h)$

*7-14.* i) $n = 1 \Rightarrow a + 1 = s(a) \neq a \neq b \neq s(b) = b + 1$

ii) $a + h \neq b + h \Rightarrow a + s(h) \neq b + s(h)$

D) $a = s(h) = s(a+h) \neq s(b+h) = b + s(h)$

*7-15.* i) 1] $n = 1 \Rightarrow 1 \,.\, 1 = 1 \,.\, 1$

2] $1 \,.\, h = h \,.\, 1 \Rightarrow 1 \,.\, s(h) = s(h) \,.\, 1$

En efecto: $1 \,.\, s(h) = 1 \,.\, h + 1 = h \,.\, 1 + 1 = h + 1 = s(h) = s(h) \,.\, 1$

ii) 1] $n = 1 \Rightarrow s(b) \,.\, 1 = 1 \,.\, s(b) = 1 \,.\, b + 1 = b \,.\, 1 + 1$

2] $s(b) \,.\, h = b \,.\, h + h \Rightarrow s(b) \,.\, s(h) = b \,.\, s(h) + s(h)$

D) $s(b) \cdot s(h) = s(b) \cdot h + s(b) = (bh + h) + s(b) =$
$= bh + (h + s(b)) = bh + (s(b) + h) = bh + s(b + h) = bh + b + s(h) =$
$= b \cdot s(h) + s(h)$
3] Es consecuencia inmediata de i ) y ii ).

*7-16.* i ) $a < b \Rightarrow b = a + x \Rightarrow bc = (a + x)c \Rightarrow$
$\Rightarrow bc = ac + xc \Rightarrow ac < bc$
ii ) $a < b \ \wedge \ c < d \Rightarrow ac < bc \ \wedge \ bc < bd \Rightarrow ac < bd$
iii) Si $a \neq 1$ entonces $1 < a$. Luego
$1 < a \Rightarrow a = 1 + x \Rightarrow ab = (1 + x)b \Rightarrow ab = b + xb \Rightarrow$
$\Rightarrow 1 = b + xb \Rightarrow b < 1$, absurdo.

*7-17.* i ) $(\mathbf{N}, *)$ no es monoide.
ii ) $(\mathbf{Z}, *)$ es monoide.
iii) $(\mathbf{R}^{2\times 2}, *)$ es monoide.

*7-18.* i ) $(a*b)*c*d = ((a*b)*c)*d =$
$= (a*(b*c))*d = a*(b*c)*d$
ii ) a) $n = 1 \Rightarrow a^m * a^1 = a^m * a = a^{m+1}$
b) $a^m * a^h = a^{m+h} \Rightarrow a^m * a^{h+1} = a^m * a^h * a =$
$= a^{m+h} * a = a^{m+h+1}$

*7-19.* Sea $S = \{S_i / i \in I\}$ una familia de sub-semigrupos de A y sea $X = \bigcap_{i \in I} S_i$ la intersección de dicha familia.

Consideramos $a \in X \ \wedge \ b \in X \Rightarrow a \in S_i \ \wedge \ b \in S_i, \forall i \in I \Rightarrow$
$\Rightarrow a * b \in S_i, \forall i \in I \Rightarrow a * b \in X$
Luego X es un subsemigrupo de A.

*7-20.* i ) Probar que $\overline{S}$ es el conjunto de los múltiplos naturales de 1, o sea
$S = \{1 \cdot a \ / \ a \in \mathbf{N}\}$
ii ) Demostrar que $S = \{1 \cdot a + (-1) \cdot b \ / \ a \in \mathbf{N}\}$, definiendo $1 \cdot a = 1$ si $a = 1$
y $1 \cdot a = \underbrace{1 + 1 + \ldots + 1}_{a}$

## TRABAJO PRACTICO VIII

*8-22.* a) No. b) Sí. c) No. d) Sí.

*8-23.* i ) Un generador es $i$.

ii ) Un generador es $z$ (obsérvese que $z^2 = \bar{z}$).

*8-24.* El neutro es $e = \frac{1}{2}$ , y el inverso de $a$ es $a' = \frac{1}{a}$

*8-25.* El neutro es $e = i$, y el inverso de $a$ es $a' = 2i - a$.

*8-26.* Está tratado en 5-31.

*8-27.* Neutro es $(0,0, \ldots, 0)$ y $(-x_1, -x_2, \ldots, -x_n)$ es el inverso aditivo de $(x_1, x_2, \ldots, x_n)$.

*8-28.* Sean $f_0$, $f_{120}$, $f_{240}$ las rotaciones de 0°, 120° y 240° respectivamente; $f_A$, $f_B$ y $f_C$ las simetrías respecto de BC, AC y AB. Proceder como en el caso 5-23.

*8-29.* Tener en cuenta 8.14.3. para obtener los subgrupos

$$H_1 = \{f_0\},\ H_2 = \{f_0, f_A\},\ H_3 = \{f_0, f_B\},\ H_4 = \{f_0, f_C\},$$

$$H_5 = \{f_0, f_{120}, f_{240}\},\ H_6 = G.$$

*8-30.* Como $(0, 0, \ldots, 0) \in H$, es $H \neq \phi$; y por definición de H se verifica $H \subset G$.

Sean $(x_1, x_2, \ldots, x_n) \in H \ \wedge\ (y_1, y_2, \ldots, y_n) \in H \Rightarrow x_i = 0 \ \wedge\ y_i = 0 \Rightarrow$

$\Rightarrow x_i - y_i = 0 \Rightarrow x_i + (-y_i) = 0 \Rightarrow$

$\Rightarrow (x_1, x_2, \ldots, x_n) + (-y_1, -y_2, \ldots, -y_n) \in H$.

Luego, $(H, +)$ es subgrupo de $(R^n, +)$.

*8-31.* $H \neq \phi$ y $H \subset R^{2\times 2}$. Sean $A \in H \ \wedge\ B \in H \Rightarrow$

$\Rightarrow A = -A^t \ \wedge\ B = -B^t \Rightarrow A + (-B) = -A^t + B^t \Rightarrow$

$\Rightarrow A + (-B) = -(A^t - B^t) = -[A + (-B)]^t \Rightarrow$

$\Rightarrow (H, +)$ es el subgrupo de las matrices antisimétricas de $(R^{2\times 2}, +)$. Pruebe el lector que $A = -A^t \Rightarrow a_{ii} = 0$, $\forall i$.

*8-32.* i ) $f(ab) = (ab)^2 = a^2 b^2 = f(a) f(b)$

ii ) Al $N(f)$ pertenecen los elementos de A que satisfacen $x^2 = 1 \Rightarrow$

$\Rightarrow x = 1 \;\vee\; x = -1 \Rightarrow N(f) = \{-1, 1\}$.
$I(f) = \mathbf{R}^+$ pues $\forall y \in \mathbf{R}^+, \exists x = \sqrt{y} / f(x) = y$.

**8-33.** Es un morfismo biyectivo, con $N(f) = \{1\}$, $I(f) = A$.

**8-34.** Está tratado en 5-38.

**8-35.** i ) $f(e) = e' \in H \Rightarrow e \in f^{-1}(H) \Rightarrow f^{-1}(H) \neq \phi$

ii ) $f^{-1}(H) \subset G$ por definición de preimagen.

iii) $x \in f^{-1}(H) \;\wedge\; y \in f^{-1}(H) \Rightarrow f(x) \in H \;\wedge\; f(y) \in H \Rightarrow$
$\Rightarrow f(x) \in H \;\wedge\; [f(y)]' \in H \Rightarrow f(x) *' f(y') \in H \Rightarrow$
$\Rightarrow f(x * y') \in H \Rightarrow x * y' \in f^{-1}(H)$.

**8-36.** $x \in G \Rightarrow x * x = x \Rightarrow x * x * x^{-1} = x * x^{-1} \Rightarrow x * e = e \Rightarrow x = e$.
Luego $G = \{e\}$.

**8-37.** Sean $a$ y $b$ en G. Se tiene:
$(a*b) * (a*b) = e = e * e = (a*a) * (b*b) \Rightarrow$
$\Rightarrow \not{a} * (b*a) * \not{b} = \not{a} * (a*b) * \not{b} \Rightarrow b * a = a * b$

**8-38.** i ) $f_a$ es morfismo, pues: $f_a(x*y) = a^{-1} * (x*y) * a =$
$= a^{-1} * x * (a * a^{-1}) * y * a = (a^{-1} * x * a) * (a^{-1} * y * a) = f_a(x) * f_a(y)$

ii ) $f$ es $1-1$. Sean $x$ e $y$ tales que $f_a(x) = f_a(y)$
Entonces $\not{a}^{-1} * x * \not{a} = \not{a}^{-1} * y * \not{a} \Rightarrow x = y$

iii) $f$ es sobreyectiva, pues $\forall y \in G, \exists x = a * y * a^{-1}$ tal que $f(x) = y$.

**8-39.** Sean $f: G \to G'$ y $g: G' \to G''$ homomorfismos respecto de $*$, $*'$ y $*''$. Entonces $g \circ f: G \to G''$ verifica

$(g \circ f)(a*b) = g[f(a*b)] = g[f(a) *' f(b)] =$
$= g[f(a)] *'' g[f(b)] = (g \circ f)(a) *'' (g \circ f)(b)$.

**8-40.** $F(a*b) = f_{a*b} = f_b \circ f_a = F(b) \circ F(a)$
En efecto: $f_{a*b}(x) = (a*b)^{-1} * x * (a*b) =$
$= b^{-1} * a^{-1} * x * a * b = b^{-1} * f_a(x) * b = f_b[f_a(x)] = (f_b \circ f_a)(x)$

**8-41.** i ) Verificar los axiomas de grupo.

ii ) Sea $*$ conmutativa. Entonces $a \circ b = b * a = a * b = b \circ a \Rightarrow \circ$ es conmutativa, y recíprocamente.

**8-42.** i ) $f$ es un morfismo, ya que $f(a*b) = (a*b)' = b' * a' = a' \circ b' = f(a) \circ f(b)$

ii ) $f$ es $1-1$, pues si $f(x) = f(y)$ entonces $x' = y' \Rightarrow x = y$.

iii) $f$ es sobreyectiva porque $\forall y \in G, \exists x = y' \in G$ tal que $f(x) = y$
El grupo $(G, \circ)$ se llama recíproco de $(G, *)$.

**8-43.** Neutro es $e = (1, 0)$, pero los pares del tipo $(0, b)$ carecen de inverso. No es grupo.

*8-44.* i ) $e \in S \wedge e \in T \Rightarrow e = e + e \in S + T \Rightarrow S + T \neq \phi$

ii ) $S + T \subset G$ por definición de $S + T$

iii) $a \in S + T \wedge b \in S + T \Rightarrow a = x + y \wedge b = z + u \;/\; x \in S, z \in S, y \in T,$
$u \in T \Rightarrow x - z \in S \wedge y - u \in T \Rightarrow (x-z) + (y-u) \in S + T \Rightarrow$
$\Rightarrow (x+y) - (z+u) \in S + T$

*8-45.* Ver *8-36*.

*8-46.* 1. Si $(X, *)$ es un grupo, entonces las ecuaciones $x * a = b$ y $a * x = b$ admiten las soluciones únicas $x = b * a^{-1}$ y $x = a^{-1} * b$.

2. Sea $(X, *)$ un semigrupo en el cual son resolubles las ecuaciones $x * a = b$ y $a * x = b$, cualesquiera que sean $a$ y $b$ en X. Entonces se verifica la existencia de un elemento $e \in X$ tal que $e * a = a$. Sea $x \in X$; por hipótesis, existe $y \in X$ de modo que $a * y = x$.
Luego

$$e * x = e * (a*y) = (e*a) * y = a * y = x$$

O sea, $e$ es neutro a izquierda.
Sea $x \in X$. Por hipótesis, existe $c \in X$ tal que $c * x = e$ y en consecuencia $c$ es inverso a izquierda de $x \in X$. El lector puede probar que la existencia de neutro y de inversos a izquierda implica que $(X, *)$ es grupo.

*47.* Aplicar 5.4.2.

*48.* i ) $f(x+y) = a^{x+y} = \underbrace{a * a * \ldots * a}_{x+y} = a^x * a^y = f(x) * f(y)$

ii ) $I(f) = \{f(x) \;/\; x \in Z\} = \{a^x \;/\; x \in Z \wedge a \in G\} = \overline{\{a\}}$

*9.* i ) $f[(x_1, x_2, x_3) + (y_1, y_2, y_3)] = f(x_1 + y_1, x_2 + y_2, x_3 + y_3) =$
$= (x_1 + y_1 - x_3 - y_3, x_2 + y_2 - x_3 - y_3) = (x_1 - x_3, x_2 - x_3) + (y_1 - y_3, y_2 - y_3) =$
$= f(x_1, x_2, x_3) + f(y_1, y_2, y_3)$

ii ) $(x_1, x_2, x_3) \in N(f) \Leftrightarrow f(x_1, x_2, x_3) = (0,0) \Leftrightarrow (x_1 - x_3, x_2 - x_3) = (0,0) \Leftrightarrow$
$\Leftrightarrow x_1 - x_3 = 0 \wedge x_2 - x_3 = 0 \Leftrightarrow x_1 = x_3 \wedge x_2 = x_3 \Leftrightarrow x_1 = x_2 = x_3$
O sea $N(f) = \{(\alpha, \alpha, \alpha) \;/\; \alpha \in \mathbf{R}\}$

iii) $I(f) = \{f(x_1, x_2, x_3) \;/\; (x_1, x_2, x_3) \in \mathbf{R}^3\}$
$\Rightarrow I(f) = \{(x_1 - x_3, x_2 - x_3) \;/\; (x_1, x_2, x_3) \in \mathbf{R}^3\}$
$(x_1 - x_3, x_2 - x_3) = (y_1, y_2) \Rightarrow x_1 - x_3 = y_1 \wedge x_2 - x_3 = y_2 \Rightarrow$
$\Rightarrow x_1 = y_1 + \alpha, x_2 = y_2 + \alpha, x_3 = \alpha$ con $\alpha \in \mathbf{R}$
O sea $I(f) = \mathbf{R}^2$

*9.* i ) Sean $H \subset G$ un subgrupo normal y $u \in G$.
$\forall a \in H : u * a * u^{-1} \in H$. Entonces $b = u * a * u^{-1} \Rightarrow u * a = b * u \Rightarrow$
$\Rightarrow u * a \in H u \Rightarrow u H \subset H u$ (1)
Sea $v = u^{-1} \Rightarrow c = v * a * v^{-1} \in H$.

Como $c = u^{-1} * a * u$, se tiene $a * u = u * c$, o sea $a * u \in u\,H \Rightarrow$
$\Rightarrow H\,u \subset u\,H$ (2)
De (1) y (2) resulta $u\,H = H\,u$.

ii) Como $u * a \in u\,H \wedge u\,H = H\,u$, se tiene $u * a \in H\,u$ y en consecuencia existe $b \in H$ tal que $u * a = b * u$. Luego $u * a * u^{-1} = b \in H$, y H es normal.

*8-51.* $f$ no es un homomorfismo.

*8-52.* i ) Sean H normal y $f_a$ un automorfismo interior de G.

$$f_a(H) = \left\{ f_a(x) \ / \ x \in H \right\} = \left\{ y = a * x * a^{-1} \ / \ x \in H \right\} = \left\{ y \ / \ y \in H \right\}$$

## TRABAJO PRACTICO IX

***9-10.*** Analizar los axiomas siguiendo el método habitual. ($\mathbf{Z}^2$ , + , ·) es anillo conmutativo, sin identidad, con divisores de cero.

***9-11.*** i ) Asociatividad: $(ab)\,c = 0\,c = 0 = a\,0 = a\,(bc)$

ii ) Distributividades: $(a+b)\,c = 0 = 0 + 0 = ac + bc$. Análogamente $c\,(a+b) = = ca + cb$.

***9-12.*** Seguir el procedimiento indicado en ejemplos anteriores. Neutro es (1,0).

***9-13.*** Considerar el ejemplo 5-7. No tiene divisores de cero.

***9-14.*** i ) $f$ es un morfismo, pues:

1. $f\,[(a+b\sqrt{2}) + (c+d\sqrt{2})] = f\,[(a+c) + (b+d)\sqrt{2}] =$
$= (a+c) - (b+d)\sqrt{2} = (a-b\sqrt{2}) + (c-d\sqrt{2}) = f\,(a+b\sqrt{2}) +$
$+ f\,(c+d\sqrt{2})$
2. $f\,[(a+b\sqrt{2})\ \ (c+d\sqrt{2}\ ] = f\,[(ac+2\,bd) + (ad+bc)\sqrt{2}] =$
$= (ac+2\,bd) - (ad+bc)\sqrt{2}$
$f\,(a+b\sqrt{2})\,.\,f\,(c+d\sqrt{2}) = (a-b\sqrt{2})\,(c-d\sqrt{2}) =$
$= (ac+2\,bd) - (ad+bc)\sqrt{2}.$

ii ) $f$ es biyectiva.

***9-15.*** Verificar los axiomas.

***9-16.*** i ) $0 \in A_1 \ \wedge\ 0 \in A_2 \Rightarrow 0 \in A_1 \cap A_2 \Rightarrow A_1 \cap A_2 \neq \phi$

ii ) $A_1 \subset A \ \wedge\ A_2 \subset A \Rightarrow A_1 \cap A_2 \subset A$

iii) $a \in A_1 \cap A_2 \ \wedge\ b \in A_1 \cap A_2 \Rightarrow a + b' \in A_1 \ \wedge\ a + b' \in A_2 \Rightarrow$
$\Rightarrow a + b' \in A_1 \cap A_2$
Esto prueba que ($A_1 \cap A_2$ , + ) es subgrupo de (A , + )

iv) El producto es ley interna en A, pues $a \in A_1 \cap A_2 \ \wedge\ b \in A_1 \cap A_2 \Rightarrow$
$\Rightarrow a\,b \in A_1 \ \wedge\ a\,b \in A_2 \Rightarrow a\,b \in A_1 \cap A_2$.

v ) La asociatividad y distributividades se verifican por ser $A_1 \cap A_2 \subset A$.

***9-17.*** Si en A existiera $x \neq 0$ tal que $x^n = 0$ o sea $x\,.\,x\,.\,.\,.\,x = 0$, entonces habría divisores de cero, lo que es absurdo.

***9-18.*** i ) Sea $a \sim b$ módulo $n \Rightarrow n | a - b \Rightarrow a - b = nk$ (1)

Además $b = nq + r \ \wedge \ 0 \leq r < n$. Sustituyendo en (1): $a - nq - r = nk \Rightarrow$
$\Rightarrow a = (k+q)n + r \ \wedge \ 0 \leq r < n$. O sea, $r$ es el resto de la división de $a$ por $n$.

ii ) Sean $a$ y $b$ tales que $a = nq + r \ \wedge \ b = nq' + r \Rightarrow a - b = n(q - q') \Rightarrow$
$\Rightarrow n | a - b \Rightarrow a \sim b$.

*9-19.* i ) $a \leq b \Rightarrow 0 \leq b - a \Rightarrow -b + 0 \leq (-b+b) - a \Rightarrow -b \leq -a$

ii ) $a = 0 \Rightarrow a^2 = 0 \Rightarrow 0 \leq a^2$
$a \in A^+ \Rightarrow a^2 \in A^+ \Rightarrow 0 < a^2 \Rightarrow 0 \leq a^2$
$a \in A^- \Rightarrow a^2 \in A^+ \Rightarrow 0 \leq a^2$
Tener en cuenta 9.8

*9-20.* i ) Se sabe que $|a + b| \leq |a| + |b|$
Sea $x - y = z \Rightarrow x = z + y \Rightarrow |x| = |z + y| \Rightarrow |x| \leq |z| + |y| \Rightarrow$
$\Rightarrow |x| - |y| \leq |z| \Rightarrow |x| - |y| \leq |x - y| \Rightarrow |x - y| \geq |x| - |y|$

ii )Por un error tipográfico, el enunciado se corrige así $||x| - |y|| \leq |x - y|$.
Utilizar i ) y 9.12.2.

iii) $x | y \ \wedge \ y \neq 0 \Rightarrow y = xk \ \wedge \ k \neq 0 \Rightarrow |y| = |x||k| \ \wedge \ |k| \geq 1 \Rightarrow$
$\Rightarrow |y||k| \geq |x||k| \Rightarrow |y| \geq |x|$

*9-21.* i ) $0 \in I \Rightarrow I \neq \phi$  ii ) $x \in I \ \wedge \ y \in I \Rightarrow nx = 0 \ \wedge \ ny = 0 \Rightarrow$
$\Rightarrow nx - ny = 0 \Rightarrow n(x - y) = 0 \Rightarrow x - y \in I$

iii) $x \in I \ \wedge \ y \in I \Rightarrow nx = 0 \ \wedge \ ny = 0 \Rightarrow (nx)(ny) = 0 \Rightarrow n[n(xy)] = 0 \Rightarrow$
$\Rightarrow n(xy) = 0 \Rightarrow xy \in A$

iv) $x \in I \ \wedge \ a \in A \Rightarrow nx = 0 \ \wedge \ a \in A \Rightarrow n(xa) = 0 \ \wedge \ n(ax) = 0 \Rightarrow$
$\Rightarrow xa \in I \ \wedge \ ax \in I$

*9-22.* Sean A un anillo de división e I cualquier ideal propio no trivial. La tarea se reduce a probar que $A \subset I$ pues por definición, se sabe que $I \subset A$. Como I es no trivial, existe un elemento no nulo $a \in I$ y por ser A un anillo de división, $a$ es inversible; en consecuencia, $a\,a^{-1} = 1$ es un elemento de I.
Sea $x \in A$; como $1 \in I$, se tiene $x\,1 \in I$, y por lo tanto $x \in I$. Luego $A \subset I$.

*9-23.* i ) Teniendo en cuenta 8-27, resulta $(\mathbf{R}^4, +)$ un grupo abeliano.

ii ) El producto es ley de composición interna en $\mathbf{R}^4$ por la definición dada. Falta probar que es asociativo, que el neutro es $(1, 0, 0, 0)$, que toda cuaterna no nula tiene inverso multiplicativo (emplear los métodos habituales). La no conmutatividad se verifica con un contraejemplo.

iii) Se completa demostrando las dos distributividades del producto respecto de la suma.
Referencia: *Vectores y Tensores*, por Luis A. Santaló, pág. 87, Editorial Eudeba, 1961.

*9-24.* Sumando las ecuaciones $\bar{0}x + \bar{0}y = \bar{0}$ y el conjunto de soluciones es $\mathbf{Z}_5$.

*9-25.* Sean $a | c \ \wedge \ b | c \ \wedge \ \text{mcd}(a, b) = 1$ ; $a | c \Rightarrow c = ax$ (1)

Por hipótesis y (1) es $b|ax$. Por 9-8 ii ) se deduce $b|x$, o sea $x = by$. Sustituyendo en (1) queda $c = (ab)\,y \Rightarrow ab|c$.

*9-26.* Sean mcd $(a,b) = d \wedge a|c \wedge b|c$. Entonces $d = sa + tb \wedge c = ax = by$. Luego $dc = saby + tbax = (sy + tx)\,ab \Rightarrow ab|dc$

*9-27.* i ) $2|10 \Rightarrow 2|10\,d$. Como $2|u$, resulta $2|10\,d + u$, o sea $2|n$.

ii ) $3|9 \Rightarrow 3|9\,d$. Como $3|d + u$, se tiene $3|9\,d + d + u$, es decir $3|10\,d + u$. Luego $3|n$.

iii) $11|11\,d \wedge 11|d - u \Rightarrow 11|11\,d - (d - u) \Rightarrow 11|10\,d + u \Rightarrow 11|n$.
Por ejemplo, si $n = 132$ como $11|13 - 2$ resulta $11|132$.

*9-28.* i ) 2 ; ii ) 5 ; iii) 21 ; iv) 5

*9-29.* $a|b \Rightarrow b = ax \Rightarrow |b| = |a|\,|x| = a\,|x|$ pues $a > 0$ ya que $|b| < a$, o sea $a > |b| \geq 0$.

De $|b| = a\,|x| \wedge a > |b|$ resulta $a > a\,|x| \Rightarrow |x| < 1 \Rightarrow x = 0$. Luego $b = ax = 0$.

*9-30.* Supongamos que $a = bq + r \wedge 0 \leqslant r < b$ y $a = bq' + r' \wedge 0 \leqslant r' < b$. Entonces $bq + r = bq' + r'$ y $b\,(q - q') = r' - r \Rightarrow b|r' - r$ (1)

Por otra parte $r' < b \wedge r \geqslant 0 \Rightarrow r' - r < b$ (2)

Además $r < b \wedge r' \geqslant 0 \Rightarrow r - r' < b$ (3)

De (2) y (3) resulta $|r' - r| < b$. (4)

De acuerdo con 9-29, de (1) y (4) se deduce $r' - r = 0$, sea $r' = r$. Entonces $b\,(q - q') = r' - r = 0 \Rightarrow q - q' = 0 \Rightarrow q' = q$.

*9-31.* El algoritmo de Euclides se reduce a

| | | | |
|---|---|---|---|
| | $q_1$ | $q_2$ | $q_3$ |
| $a$ | $b$ | $r_1$ | $r_2$ |
| $r_1$ | $r_2$ | 0 | |

mcd $(a\,,\,b) = r_2$. Por el algoritmo de la división entera, se tiene

$$a = b\,q_1 + r_1 \quad \text{y} \quad b = r_1\,q_2 + r_2 \Rightarrow r_2 = b - r_1\,q_2 = b - q_2\,(a - b\,q_1) =$$
$$= b - q_2\,a + q_1\,q_2\,b = (-q_2)\,a + (1 + q_1\,q_2)\,b$$

*9-32.* Mediante 9-26, como mcd $(a\,,\,b) = d$, $a|m$ y $b|m$, resulta $ab|dm$. Probar que $dm|ab$.

*9-33.* $a \sim b \Rightarrow n \mid a-b \Rightarrow a-b=nh \Rightarrow a=b+nh \Rightarrow a^k = (b+nh)^k =$
$= b^k + \sum_{i=1}^{k} \binom{k}{i} b^{k-i} n^i h^i \Rightarrow a^k - b^k = n \sum_{i=1}^{k} \binom{k}{i} b^{k-i} n^{i-1} h^i = nq \Rightarrow$
$\Rightarrow n \mid a^k - b^k \Rightarrow a^k \sim b^k$

*9-34.* En 5-8 está comprobado que $(\mathbf{R}^{n\times n}, +)$ es grupo abeliano. Verificamos entonces
$A_6$: El producto es ley de composición interna en $\mathbf{R}^{n\times n}$, de acuerdo con 9-2.

$A_7$: Asociatividad. Sean A, B y C en $\mathbf{R}^{n\times n}$, y los productos A (BC) y A (BC).
La fila $i$ de A es: $a_{i1}, a_{i2}, \ldots, a_{in}$. La columna $j$ de BC es

$$\sum_{k=1}^{n} b_{1k}\, c_{kj}, \sum_{k=1}^{n} b_{2k}\, c_{kj}, \ldots, \sum_{k=1}^{n} b_{nk}\, c_{kj}$$

Entonces el elemento $(i, j)$ de A (BC) es $\sum_{h=1}^{n} a_{ih} \sum_{k=1}^{n} b_{hk}\, c_{kj} =$

$= \sum_{h=1}^{n} \sum_{k=1}^{n} a_{ih}\, b_{hk}\, c_{kj} = \sum_{k=1}^{n} \left( \sum_{h=1}^{n} a_{ih}\, b_{hk} \right) c_{kj}$ que es el elemento $(i, j)$ de (AB) C.

$A_8$: El elemento genérico de I es $\delta_{ij}$ (delta de Kronecker) definido por $\delta_{ij} = 0$ si $i \neq j$ y $\delta_{ij} = 1$ si $i = j$. El elemento $(i, j)$ de A I es $\sum_{k=1}^{n} a_{ik}\, \delta_{kj} = a_{i1}\, \delta_{1j} + a_{i2}\, \delta_{2j} + \ldots + a_{ij}\, \delta_{jj} + \ldots + a_{in}\, \delta_{nj} = a_{ij}\, 1 = a_{ij} \Rightarrow \text{A I} = \text{A}$, y análogamente I A = A.

$A_9$: Sea C (A + B). La fila $i$ de C es: $c_{i1}, c_{i2}, \ldots, c_{in}$.
La columna $j$ de A+ B es: $a_{1j} + b_{1j}, a_{2j} + b_{2j}, \ldots, a_{nj} + b_{nj}$.

Entonces, el elemento $(i, j)$ de C (A + B) es $\sum_{k=1}^{n} c_{ik}\, (a_{kj} + b_{kj}) =$
$= \sum_{k=1}^{n} c_{ik}\, a_{kj} + \sum_{k=1}^{n} c_{ik}\, b_{kj}$, que corresponde al elemento $(i, j)$ de CA + CB.

O sea C (A + B) = CA + CB. Análogamente se prueba (A + B) C = AC + BC.

*9-35.* Hipótesis) Para cada $m$ se verifica

$$\forall\, h < m : \text{P}(h) \text{ es V} \Rightarrow \text{P}(m) \text{ es V}$$

Tesis) P $(m)$ es V, $\forall\, n \in \mathbf{N}$

Demostración)

Suponemos que $\text{H} = \{x \in \mathbf{N} \;/\; \text{P}(x) \text{ es F}\} \neq \phi$. Por el principio de buena ordenación, existe en H el elemento mínimo $m$, tal que P $(m)$ es F (1), y $h < m \Rightarrow \text{P}(h)$ es V. Ahora bien, por hipótesis resulta P $(m)$ es V, lo que es contradictorio con (1), o sea $\text{H} = \phi$.

*9-36.* $ac \sim bc \Rightarrow n | ac - BC \Rightarrow n | (a-b)\, c \Rightarrow n | a-b$ (porque si un entero es divisor de un producto y es primo con uno de los factores, entonces es divisor del otro). Luego $a \sim b$.

**9-37.** i ) Sean $\left\{a_1, a_2, \ldots, a_n\right\}$ una clase completa de residuos módulo $n$ y $a_i \neq a_j$. Si $a_i \sim a_j$, entonces $a_i$ y $a_j$ pertenecen a la misma clase de equivalencia, lo que es contradictorio con la hipótesis.
Recíprocamente, si $a_i \nsim a_j$, $\forall i \neq j$, entonces dos elementos cualesquiera y distintos no pertenecen a la misma clase de equivalencia, y en consecuencia $\left\{a_1, a_2, \ldots, a_n\right\}$ es una clase completa de residuos módulo $n$.

ii ) En efecto, supongamos que $aa_i \sim aa_j$ para algún $i \neq j$. Entonces $n | aa_i - aa_j$, o sea $n | a(a_i - a_j)$, y como $a$ y $n$ son coprimos, se deduce que $n | a_i - a_j$, es decir $a_i \sim a_j$. Esto es contradictorio con la hipótesis.

**9-38.** Sea la clase de restos módulo $p$ : $0, 1, \ldots, p-1$. Como $a \neq 0$ ya que $a$ no es múltiplo de $p$, $a0, a1, a2, \ldots, a(p-1)$ constituyen una clase completa de restos módulo $p$, por 9-38 ii ). Entonces cada elemento de la primera clase es equivalente a uno de la segunda, y recíprocamente. Como 0 pertenece a las dos, por la compatibilidad de la relación respecto del producto, se tiene

$$1 . 2 \ldots (p-1) \sim (a\,1)(a\,2) \ldots (a\,(p-1))$$

O sea $(p-1)! \sim a^{p-1}\,(p-1)!$, o lo que es lo mismo, $p | (a^{p-1} - 1)(p-1)!$.
Como $p$ y $(p-1)!$ son coprimos, resulta $p | (a^{p-1} - 1) \Rightarrow a^{p-1} \sim 1$.

**9-39.** i ) $a$ y $n$ son coprimos $\Rightarrow mcd\,(a,n) = 1 \Rightarrow 1 = s\,a + t\,n \Rightarrow b = s\,a\,b + t\,n\,b \Rightarrow$ $\Rightarrow b - (sb)\,a = (tb)\,n \Rightarrow n \mid b - (sb)\,a \Rightarrow a\,(sb) \sim b \Rightarrow s\,b$ es solución de la ecuación.

ii ) Sean $s_1$ y $s_2$ soluciones de $ax \equiv b$ (mód. $n$). Entonces $as_1 \sim b \;\wedge\; as_2 \sim b \Rightarrow$ $\Rightarrow as_1 \sim as_2$, por la simetría y transitividad de la relación. Se tiene $n | a\,(s_1 - s_2)$ y $a$ coprimo con $n \Rightarrow n | s_1 - s_2 \Rightarrow s_1 \sim s_2$.

iii) Siendo $a$ y $n$ coprimos, y $n$ primo, por 9-38 se tiene $a^{n-1} \sim 1 \Rightarrow$ $\Rightarrow a^{n-1}\,b \sim b \Rightarrow aa^{n-2}\,b \sim b \Rightarrow x = a^{n-2}\,b$ es solución de $ax \sim b$ (mód. $n$).

**9-40.** i ) Como 3 y 4 son coprimos, es mcd $(3\;,4) = 1 = (-1)\,3 + 1 . 4 \Rightarrow$ $\Rightarrow sb = (-1)\,7 = -7$ es solución. Todos los congruentes a $-7$ módulo 4, son soluciones (ver 9-39).

ii ) $12 | x - 6 \Rightarrow x = 6 + 12\,k \;\wedge\; k \in \mathbf{Z}$ son soluciones.

iii) De acuerdo con 9-36, $-2\,x \sim 12 \Rightarrow x \sim -6$ luego de cancelar $-2$, que es coprimo con 11. Por 9-39 iii) es $x = 1^{11-2}\;.(-6) = -6$ una solución. Resulta $K_5$ el conjunto de las soluciones

**9-41.** i ) $\frac{a}{b} + \frac{c}{d} = ab^{-1} + cd^{-1} = ab^{-1}\,d^{-1}\,d + cd^{-1}\,b^{-1}\,b = (ad+bc)\,(bd)^{-1} =$

$$= \frac{a\,d + b\,c}{b\,d}$$

ii) $\frac{a}{b} \cdot \frac{c}{d} = a\,b^{-1}\,c\,d^{-1} = (ac)\,(bd)^{-1} = \frac{a\,c}{b\,d}$

iii) $\frac{a}{b} = \frac{c}{d} \Rightarrow \frac{a}{b} + \frac{b}{b} = \frac{c}{d} + \frac{d}{d} \Rightarrow \frac{a+b}{b} = \frac{c+d}{d}$

**9-42.** Sean $K_1$ y $K_2$ subcuerpos de K. Como $1 \in K_1 \ \wedge \ 1 \in K_2$, es $1 \in K_1 \cap K_2$, o sea $K_1 \cap K_2 \neq \phi$. Además $K_1 \subset K \ \wedge \ K_2 \subset K \Rightarrow K_1 \cap K_2 \subset K$. Mediante la condición suficiente 8.4.2., el lector puede demostrar que $(K_1 \cap K_2, +)$ y $((K_1 \cap K_2) - \{0\}, .)$ son subgrupos de $(K, +)$ y de $(K - \{0\}, .)$, respectivamente. La distributividad es consecuencia de que $K_1 \cap K_2 \subset K$.

**9-43.** i) $n = 1 \Rightarrow x^1 + y^1 = x + y = \frac{(x+y)^1}{2^{1-1}}$

ii) $x^h + y^h \geqslant \frac{(x+y)^h}{2^{h-1}} \Rightarrow x^{h+1} + y^{h+1} \geqslant \frac{(x+y)^{h+1}}{2^h}$

En efecto, $(x^h - y^h)(x - y) \geqslant 0 \Rightarrow x^{h+1} + y^{h+1} - y\,x^h - x\,y^h \geqslant 0 \Rightarrow$
$\Rightarrow x\,y^h + x^h\,y \leqslant x^{h+1} + y^{h+1} \Rightarrow x^{h+1} + x\,y^h + x^h\,y + y^{h+1} \leqslant 2\,x^{h+1} +$
$+ 2\,y^{h+1} \Rightarrow x\,(x^h + y^h) + y\,(x^h + y^h) \leqslant 2\,(x^{h+1} + y^{h+1}) \Rightarrow$
$\Rightarrow (x+y)\,(x^h + y^h) \leqslant 2\,(x^{h+1} + y^{h+1})$

Por la hipótesis inductiva

$$x^{h+1} + y^{h+1} \geqslant (x^h + y^h)\,\frac{x+y}{2} \geqslant \frac{(x+y)^h}{2^{h-1}}\,\frac{x+y}{2} = \frac{(x+y)^{h+1}}{2^h}$$

**9-44.** $(Q(\sqrt{3}), +, .)$ es un subcuerpo de $(R, +, .)$. Basta probar que $(Q(\sqrt{3}), +)$ y $(Q(\sqrt{3}) - \{0\}, .)$ son subgrupos de $(R\ +)$ y de $(R - \{0\}, .)$, respectivamente. (Ver 5-7).

**9-45.** i) $(nx)(my) = \underbrace{(x + x + \ldots + x)}_{n}\underbrace{(y + y + \ldots + y)}_{m} = \underbrace{xy + xy + \ldots + xy}_{nm} =$
$= (nm)(xy)$

ii) $(ne)(me) = (nm)(ee) = (nm)\,e$

**9-46.** i) $p\,x = (p\,1)(ex) = (pe)(1x) = 0x = 0$

Debe notarse que $p$ y $1$ son elementos de N y no de K.

ii) Si $p$ no fuera primo, admitiría la descomposición $p = p_1\,p_2$, con $1 < p_1 < p$ y $1 < p_2 < p$.

Entonces $p\,e = (p_1\,p_2)\,e = (p_1\,p_2)(e\,e) = (p_1\,e)(p_2\,e) = 0$. Y como no existen divisores de cero, resulta $p_1\,e = 0 \ \vee \ p_2\,e = 0$; o sea, la característica es $p_1$ o $p_2$, lo que es contradictorio con la hipótesis.

**9-47.** $(x + y)^p = x^p + \sum_{i=1}^{p} \binom{p}{i} x^{p-i}\,y^i + y^p$. Todo término del desarrollo de la sumatoria tiene coeficiente $\binom{p}{i} = \frac{p\,(p-1)\ldots(p-i+1)}{i!}$, donde la

característica $p$ es un factor. Por 9-46 i ), tales términos se anulan y resultan $(x=y)^p = x^p + y^p$

*9-48.* i ) El conjunto $\left\{x \in Q^+ / x^2 < 2\right\}$ carece de supremo en Q.

ii ) Sean $x = \frac{p}{q}$ e $y = \frac{r}{s}$. Tomando $n \geq qr$ se tiene $nps \geq qr \Rightarrow$

$$\Rightarrow nps - qr \geq 0 \Rightarrow \frac{nps-qr}{qs} \geq 0 \Rightarrow n\,\frac{p}{q} - \frac{r}{s} \geq 0 \Rightarrow nx \geq \frac{r}{s}$$

*9-49.* Ver 6-66 y 6-67.

*9-50.* i ) Sean $A_i = a_{i1}, a_{i2}, \ldots, a_{in_i}$ con $i \in N$, tales que $i \neq j \Rightarrow A_i \cap A_j = \phi$. Definimos

$$f: \sum_{i=1}^{\infty} A_i \to N \text{ mediante}$$

$f(a_{ij}) = \sum_{h=1}^{i-1} n_h + j$. Como $f$ es biyectiva, resulta $\sum_{i=1}^{\infty} A_i$ numerable.

ii ) Sean

$$\begin{array}{lllllll} A_1: & a_{11} & a_{12} & a_{13} & \ldots & a_{1n} & \ldots \\ A_2: & a_{21} & a_{22} & a_{23} & \ldots & a_{2n} & \ldots \\ A_3: & a_{31} & a_{32} & a_{33} & \ldots & a_{3n} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

Ordenando según el proceso diagonal de Cantor, resulta $\sum_{i=1}^{\infty} A_i$ igual a la unión de una familia numerable de conjuntos finitos, que es numerable por i ).

## TRABAJO PRACTICO X

*10-8.* Sea $\frac{p}{q} \in \mathbf{Q}$ una raíz, con mcd $(p,q) = 1$. Se tiene $\left(\frac{p}{q}\right)^n + \sum_{i=0}^{n-1} a_i \left(\frac{p}{q}\right)^i = 0 \Rightarrow$

$\Rightarrow p^n + q^n \left(a_0 + a_1 \frac{p}{q} + \ldots + a_{n-1} \frac{p^{n-1}}{q^{n-1}}\right) = 0 \Rightarrow p^n + a_0 q^n +$

$+ a_1 pq^{n-1} + \ldots + a_{n-1} p^{n-1} q = 0 \Rightarrow p^n + q\,(a_0 q^{n-1} + a_1 pq^{n-2} + \ldots +$
$+ a_{n-1} p^{n-1}) = 0 \Rightarrow p^n + q\,s = 0 \Rightarrow -q\,s = p^n \Rightarrow q \mid p^n$ y siendo $p$ y $q$ coprimos, es $q \mid p$, es decir $q = \pm 1$. Luego $\frac{p}{q} \in \mathbf{Z}$.

*10- 9.* i ) Considerár la ecuación $x^2 - 5 = 0$ y verificar que carece de raíces enteras.
ii ) Si $d$ es la diagonal y $a$ la arista, se verifica $d^2 = 3a^2 \Rightarrow \left(\frac{d}{a}\right)^2 = 3$.

Haciendo $\frac{d}{a} = x$, considerar $x^2 - 3 = 0$.

*10-10.* Sea $p \in \mathbf{Z}$ raíz de la ecuación. Entonces
$p^n + a_{n-1} p^{n-1} + a_{n-2} p^{n-2} + \ldots + a_1 p + a_0 = 0 \Rightarrow$
$\Rightarrow p \,.\, s + a_0 = 0$ con $s = a_{n-1} p^{n-2} + \ldots + a_1 \Rightarrow p(-s) = a_0 \Rightarrow p \mid a_0$

*10-11.* Considerar $\frac{p}{q} \in \mathbf{Q}$ con mcd $(p,q) = 1$. Si fuera raíz, al sustituir se llega a

$\frac{p}{q} = \pm 1$ o $\frac{p}{q} = \pm \frac{1}{3}$, valores que no satisfacen a la ecuación.

*10-12.* Sea $\sqrt{2} + \sqrt{5} = x \Rightarrow 2 + 5 + 2\sqrt{10} = x^2 \Rightarrow 2\sqrt{10} = x^2 - 7 \Rightarrow x^4 - 14x^2 + 9 = 0$ tiene como raíz a $\sqrt{2} + \sqrt{5}$, pero carece de raíces enteras.

*10-13.* En efecto $\forall_i \; \forall_j$ se verifica:

$$a_i = 3 < 3 + \frac{1}{10^j} = b'_j \quad \text{y} \quad b_j = 3 - \frac{1}{10^j} < 3 + \frac{1}{10^i} = a'_i$$

*10-14.*

$$\text{Para } \sqrt{2}: \begin{cases} 1 & 1{,}4 & 1{,}41 \\ 2 & 1{,}5 & 1{,}42 \end{cases}$$

$$\text{Para } \sqrt{3}: \begin{cases} 1 & 1{,}7 & 1{,}73 \\ 2 & 1{,}8 & 1{,}74 \end{cases}$$

Resulta:

$\sqrt{2}+\sqrt{3}:\begin{cases} 2 & 3,1 & 3,14 \\ 4 & 3,3 & 3,16 \end{cases}$

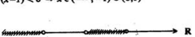
$\sqrt{2}-\sqrt{3}:\begin{cases} -1 & -0,4 & -0,33 \\ 1 & -0,3 & -0,31 \end{cases}$

$\sqrt{2}.\sqrt{3}:\begin{cases} 1 & 2,38 & 2,4393 \\ 4 & 2,70 & 2,4708 \end{cases}$

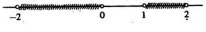
Para $\sqrt{2}:\sqrt{3}$, obtener $\dfrac{1}{\sqrt{3}}$ como se indica en 10.3 .

***10-15.*** i ) $A = Q^- \cup \{0\} \cup \{x \in Q^+ \ / \ x^2 < 3\}$
ii ) $A = Q^- \cup \{0\} \cup \{x \in Q^+ \ / \ x^2 < 5\}$

***10-16.*** i ) $[-4, 0]$ ii ) $(-\infty, -3) \cup (-1, +\infty)$
iii) $(-\sqrt{5}, \sqrt{5})$ iv) $(-\infty, -\sqrt{5}) \cup (\sqrt{5}, +\infty)$
v ) De $x^3 < x$ resulta
$x(x+1)(x-1) < 0 \Rightarrow x \in (-\infty, -1) \cup (0,1)$




vi) $(x+2)(x-1)(x-2)\,x < 0 \Rightarrow x \in (-2, 0) \cup (1,2)$




Extremos inferiores o ínfimos: $-4$, no tiene, $-\sqrt{5}$, no tiene, no tiene, $-2$.
Extremos superiores o supremos: 0, no tiene, $\sqrt{5}$, no tiene, 1, 2.

***10-17.*** $\sqrt{5} < \sqrt{2} + \sqrt{3}$.

***10-18.*** Cotas inferiores son los racionales menores o iguales que 0; cotas superiores son los mayores o iguales que 1. El supremo es 1 y el ínfimo es 0.

***10-19.*** i ) Cota superior es todo real mayor o igual que $\sqrt{2}$.
Cota inferior es todo real menor o igual que 0.
Supremo es $\sqrt{2}$; ínfimo es 0.

ii ) $B = (-\infty, -\sqrt{2}] \cup [\sqrt{2}, +\infty)$. No está acotado y carece de extremos.

iii) $C = [\ \sqrt{2}\ , +\infty)$. No tiene cotas ni extremo superiores; está acotado inferiormente por todo real menor o igual que $\sqrt{2}$, y el ínfimo es $\sqrt{2}$.

***10-20.*** Sea $c \in C \Rightarrow c = x + y$ con $x \leq a \ \wedge \ y \leq b \Rightarrow c \leq a + b \Rightarrow a + b$ es cota superior de C.
$\forall \ \mathcal{E} > 0, \exists x \in A \ \wedge \ \exists y \in B \ / \ a < x + \mathcal{E}, \wedge \ b < y + \mathcal{E}$, y si $c'$ es otra cota superior de C, entonces $a + b - 2 \ \mathcal{E} < x + y \leq c'$, o sea $a + b \leq c' + 2$ .
Luego $a + b \leq c'$.

***10-21.*** $3x^2 - 2x - 1 < 0 \Rightarrow 3(x-1)\left(x + \frac{1}{3}\right) < 0 \Rightarrow x \in \left(-\frac{1}{3}, 1\right)$.

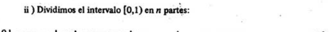
Infimo es $-\frac{1}{3}$ , y supremo es 1.

***10-22.*** Si todo $x \in A$ verifica $x \leq a - \mathcal{E} < a$, el supremo no sería $a$, lo que es absurdo.

***10-23.*** III. $\sqrt[n]{\alpha} = x \ \wedge \ \sqrt[m]{x} = y \Rightarrow \alpha = x^n \ \wedge \ x = y^m \Rightarrow \alpha = (y^m)^n = y^{mn} \Rightarrow$
$\Rightarrow y = \sqrt[mn]{\alpha}$
IV. $\sqrt[n]{\alpha^m} = x \Rightarrow \alpha^m = x^n \Rightarrow \alpha^{mp} = x^{np} \Rightarrow x = \sqrt[np]{\alpha^{mp}}$

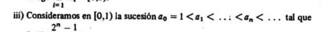
***10-24.*** i ) $(a,b) = [a,b] - \{a,b\} \sim [a,b] \sim [0,1]$
Porque la diferencia entre un conjunto no numerable y un conjunto a lo sumo numerable, es coordinable al primero.

ii ) Dividimos el intervalo $[0,1)$ en $n$ partes:




Se tiene $[0,1) = \sum_{i=1}^{n} [a_{i-1}, a_i) = \sum_{i=1}^{n} B_i$
$\forall_i = 1, 2, \ldots, n$ es $A_i \sim B_i \Rightarrow \exists f_i : A_i \to B_i$ biyectiva. Definimos
$f : \sum_{i=1}^{n} A_i \to \sum_{i=1}^{n} B_i$ mediante $f(x) = f_i(x)$ si $x \in A_i$, la que es biyectiva.
Luego $\sum_{i=1}^{n} A_i \sim [0,1)$.

iii) Consideramos en $[0,1)$ la sucesión $a_0 = 1 < a_1 < \ldots < a_n < \ldots$ tal que
$a_n = \frac{2^n - 1}{2^n}$




Se tiene $A_i \sim [a_{i-1}, a_i) \ \forall \ i \in N$ y con el mismo procedimiento utilizado en ii ) resulta $\sum_{i=1}^{\infty} A_i \sim [0,1)$.

*10-25.* i ) $2\sqrt{6}$ ii ) $\log_2 5 = \log_{1/2} \frac{1}{5}$

*10-26.* i ) $2\sqrt[4]{2}$ ii ) $\sqrt{3}+\sqrt{2}$ ; $-\frac{1}{2}(1+\sqrt{2}+\sqrt{5})(2-\sqrt{5})$

*10-27.* i ) Aplicando 10.9.2 iv)

$\cancel{\log_2 x^2} + \log_2 (2x)^3 - \cancel{\log_2 x^2} = 1$

$(2x)^3 = 2 \Rightarrow x = \frac{\sqrt[3]{2}}{2}$

ii ) $(12)^x = 11 + 1 \Rightarrow x = 1$

*10-28.* $4 \,.\, 4^y - 3 \,.\, 4^y = 1 \Rightarrow 4^y = 1 \Rightarrow y = 0$

*10-29.* $x^{\sqrt{x}} = x^{x/2} \ \wedge\ x \neq 1 \Rightarrow \sqrt{x} = \frac{x}{2} \Rightarrow 4x = x^2 \Rightarrow x = 0 \ \vee\ x = 4$

En $\mathbf{R}^+$ son soluciones 4 y 1.

*10-30.* Sustituir $\log_y x$ por $\frac{1}{\log_x y}$ en la primera ecuación y se llega a $3(\log_x y)^2 - 4\log_x y + 3 = 0$, que carece de raíces en $\mathbf{R}$ porque $\Delta = b^2 - 4ac = -20$.

Si la primera ecuación tiene segundo miembro igual a $\frac{10}{3}$, el sistema admite las soluciones (2,8) y (8,2).

# TRABAJO PRACTICO XI

*11-16.* $(8+2\sqrt{3})+(2+3\sqrt{3})i$

*11-17.* a) $z=-1-2i$ b) $z=-1+i$ c) $z=1-i$ d) $z=-2i$

*11-18.* a) $z=4i$ b) $-1+\sqrt{6}i$ c) $2\sqrt{6}+i$ d) 1

*11-19.* a) $z=-i$ b) $z=\frac{1}{2}-\frac{1}{2}i$ c) $z=-\frac{1}{5}+\frac{2}{5}i$ d) $z=-i$

*11-20.* a) $z=-\frac{1}{5}+\frac{2}{5}\sqrt{6}i$ b) $z=1-7i$ c) $z=\frac{4}{3}+\frac{2}{3}i$

*11-21.* a) $z=\pm(1+i)$ b) $z=\pm(1-2i)$ c) $z=\pm(\sqrt{2-\sqrt{3}}+i\sqrt{2+\sqrt{3}})$

*11-22.* a) $z_1=2(\cos 30^\circ+i\,\text{sen}\,30^\circ)$ b) $z_2=4(\cos 240^\circ+i\,\text{sen}\,240^\circ)$
c) $z_3=\sqrt{2}(\cos 225^\circ+i\,\text{sen}\,225^\circ)$ d) $z_4=3(\cos 270^\circ+i\,\text{sen}\,270^\circ)$

*11-23.* a) $z_1^6=-64$ b) $z_2z_3=4\sqrt{2}(\cos 105^\circ+i\,\text{sen}\,105^\circ)$
c) $\frac{z_3}{z_4}=\frac{1}{3}-\frac{1}{3}i$ d) $z_3^{10}=32i$

*11-24.* $\overline{z}^2=4i$

*11-25.* $f(\overline{z})=a\overline{z}^2+b\overline{z}+c=\overline{az}^2+\overline{bz}+\overline{c}=\overline{az^2+bz+c}=\overline{0}=0$

*11-26.* $|z^2-\overline{z}|=[(\text{sen}\,a-\cos 2a)^2+(3\cos a+\text{sen}\,2a)^2]^{1/2}$

*11-27.* $a=-\frac{2}{3}$, $b=\frac{1}{3}$

*11-28.* $1, i, -1, -i$.

*11-29.* $z_1=3, z_2=-1+2i$

*11-30.* $x=\frac{6}{13}-\frac{3}{13}i$, $y=-\frac{16}{13}+\frac{11}{13}i$

*11-31.* a) $-\overline{z}+\overline{z}=0=\overline{0}=-\overline{z+z}=\overline{-z+z}=\overline{-z}+\overline{z}$
Cancelando $\overline{z}$ resulta $-\overline{z}=-\overline{z}$
b) $\overline{z_1-z_2}=\overline{z_1+(-z_2)}=\overline{z_1}+\overline{(-z_2)}=\overline{z_1}-\overline{z_2}$

c) $|z_1| = |z_1 - z_2 + z_2| \leq |z_1 - z_2| + |z_2|$
Luego $|z_1| - |z_2| \leq |z_1 - z_2|$

d) $\overline{z_1} = \overline{\frac{z_1}{z_2}\, z_2} = \left(\overline{\frac{z_1}{z_2}}\right) \overline{z_2} \Rightarrow \frac{\overline{z_1}}{\overline{z_2}} = \left(\overline{\frac{z_1}{z_2}}\right)$

e) $z_1 = \frac{z_1}{z_2}\, z_2 \Rightarrow |z_1| = \left|\frac{z_1}{z_2}\right| |z_2| \Rightarrow \frac{|z_1|}{|z_2|} = \left|\frac{z_1}{z_2}\right|$

*11-32.* $|z^{-1} - z'^{-1}| = \left|\frac{1}{z} - \frac{1}{z'}\right| = \left|\frac{z' - z}{z \cdot z'}\right| = \frac{|z' - z|}{|z|\ |z'|} =$

$= \frac{1}{|z|}\ |z - z'|\ \frac{1}{|z'|} = |z|^{-1}\ |z - z'|\ |z'|^{-1}$

*11-33.* $|z + z'|^2 + |z - z'|^2 = (z+z')(\overline{z}+\overline{z}') + (z-z')(\overline{z}-\overline{z}') =$
$= z\overline{z} + z\overline{z}' + z'\overline{z} + z'\overline{z}' + z\overline{z} - z\overline{z}' - z'\overline{z} + z'\overline{z}' = 2\,|z|^2 + 2\,|z'|^2$

*11-34.* i ) $n = 1 \Rightarrow (\cos x + i \operatorname{sen} x)^1 = \cos x + i \operatorname{sen} x = \cos 1\,x + i \operatorname{sen} 1\,x$
ii ) $(\cos x + i \operatorname{sen} x)^h = \cos hx + i \operatorname{sen} hx \Rightarrow (\cos x + i \operatorname{sen} x)^{h+1} =$
$= \cos (h+1)\,x + i \operatorname{sen} (h+1)\,x$

**Aplicar al primer miembro de la tesis la definición de potenciación, y luego la hipótesis inductiva. Ver 11.9.3.**

*11-35.* i ) Está resuelto en 11-10.

ii ) Aplicar 11-34. y cubo de un binomio. Igualar después las partes real e imaginaria.

*11-36.* i ) Siendo 1, $w$ y $w^2$ las raíces de $x^3 - 1 = 0$, es $\overline{w} = w^2$ y además
$1 + w + w^2 = 0$. Entonces $1 + w^2 = -w \Rightarrow (1 + w^2)^4 = (-w)^4 =$
$= w^3\, w = 1\, w = w$

ii ) $(1 - w + w^2)(1 + w - w^2) = [1 + (w - \overline{w})][1 - (w - \overline{w})] =$
$= 1 - (w - \overline{w})^2 = 1 - w^2 + 2\, w\overline{w} - \overline{w}^2 = 1 - w^2 + 2\, w w^2 - w^4 =$
$= 1 - w^2 - w + 2\, w^3 = 1 + 1 + 2 = 4$

*11-37.* i ) $w = \pm (1 - 4i)$ ii ) $w = \pm (3 - 2i)$ iii) $w = \pm (\sqrt{10} + \sqrt{2}\, i)$

*11-38.* i ) $x_1 = 1 + 2i$ , $x_2 = 1 - i$ ii ) $x = \dfrac{3 - 2i \pm \sqrt{(-3 + 2i)^2 + 4i}}{2}$

*11-39.* i ) $\rho = \sqrt{2}, \varphi = 315^\circ, w_k = \sqrt[8]{2}\ \cos\left(\frac{315^\circ + 2k\pi}{4} + i \operatorname{sen} \frac{315^\circ + 2k\pi}{4}\right)$

con $k = 0, 1, 2, 3$.

ii ) $\rho = 1, \varphi = 270^\circ, w_k = \cos \frac{270^\circ + 2k\pi}{3} + i \operatorname{sen} \frac{270^\circ + 2k\pi}{3}$

con $k = 0, 1, 2$.

iii) $\rho = 8, \varphi = 0, w_k = 2\ \cos\left(\frac{2k\pi}{3} + i \operatorname{sen} \frac{2k\pi}{3}\right), k = 0, 1, 2.$

iv) $\rho = 2, \varphi = 30^\circ, w_k = \sqrt[3]{2}\ \cos\left(\frac{30^\circ + 2k\pi}{3} + i \operatorname{sen} \frac{30^\circ + 2k\pi}{3}\right), k =$
$= 0, 1, 2.$

*11-40.* i ) $\rho=\sqrt{6}$ , $\varphi=315^\circ=\frac{7}{4}\pi$ , $\ln z=\ln\sqrt{6}+i\left(\frac{7}{4}\pi+2k\pi\right)$

ii ) $\rho=e$ , $\varphi=\frac{3}{2}\pi$ , $\ln z=1+i\left(\frac{3}{2}\pi+2k\pi\right)$

iii) $\rho=4$ , $\varphi=0$ , $\ln z=\ln 4+2k\pi i$

En todos los casos $k\in\mathbf{Z}$, y el valor principal se obtiene para $k=0$.

*11-41.* i ) $\ln w=(1-i)\ln(\sqrt{2}-i)$. Para el logaritmo es $\rho=\sqrt{3}$, $\varphi=\operatorname{arc\,tg}\frac{-\sqrt{2}}{2}$ en el cuarto cuadrante.

Luego $w=e^{(1-i)\ln(\sqrt{2}-i)}$

ii ) $\ln w=2i\ln 3i=3i\left[\ln 2+i\frac{\pi}{2}\right]=$

$=-\frac{3}{2}\pi+3i\ln 2\Rightarrow w=e^{-\frac{3}{2}\pi+3i\ln 2}$

iii) $\ln w=\frac{1}{i}\ln(1-i\sqrt{3})$

$=-i\left(\ln 2+i\,11\frac{\pi}{6}\right)=11\frac{\pi}{6}-i\ln 2\Rightarrow$

$\Rightarrow w=e^{11\frac{\pi}{6}-i\ln 2}$

*11-42.* i ) $z=0$ ii ) $z\ln\left(\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)=\ln i\Rightarrow z=\frac{3}{2}$

*11-43.* i ) Resolviendo la ecuación cuadrática en $x^i$, se obtiene $x^i=1+i \vee x^i=$ $=1-i$, de donde, después de aplicar logaritmos, resulta

$x=e^{\frac{\pi}{4}-i\ln\sqrt{2}} \vee x=e^{7\frac{\pi}{4}-i\sqrt{2}}$

ii ) $x^{\sqrt{3}}=\frac{1\pm\sqrt{-3}}{2}=\frac{1\pm i\sqrt{3}}{2}\Rightarrow x^{\sqrt{3}}=\frac{1}{2}+i\frac{\sqrt{3}}{2}\vee$

$x^{\sqrt{3}}=\frac{1}{2}-i\frac{\sqrt{3}}{2}\Rightarrow x=e^{\frac{\pi\sqrt{3}}{9}i} \vee x=e^{\frac{5\pi\sqrt{3}}{9}i}$

*11-44.* i ) Es la recta $x=-2$

ii ) $\{(x,y)\,/\,-2\leqslant y<3\}$

iii) $|z+1|>2\Rightarrow(x+1)^2+y^2>4$. Es el exterior de la circunferencia de centro $(-1,0)$ y radio 2.

iv) $\left\{(x,y)\,/\,-\frac{1}{2}<x<\frac{1}{2} \wedge x^2+y^2=4\right\}$

v) $\{(\varphi, \rho) / 45° \leq \varphi \leq 135° \ \wedge \ \rho < 2\}$

vi) $|x + yi - 1 + i| = 2 \Rightarrow (x-1)^2 + (y+1)^2 = 4$. Es la circunferencia de centro $(1, -1)$ y radio 2.

*11-45.* i ) $|z+1|^2 = (x+1)^2 + y^2$ (1), $|z-1|^2 = (x-1)^2 + y^2$. Restando estas igualdades: $|z+1|^2 - |z-1|^2 = 4x \Rightarrow$

$$\Rightarrow 3(|z+1| - |z-1|) = 4x \Rightarrow |z+1| - |z-1| = \frac{4}{3}x \quad (2)$$

Como $|z+1| + |z-1| = 3$ (3), sumando (2) y (3) se tiene $|z+1| = \frac{3}{2} + \frac{2}{3}x$, que sustituido en (1) conduce a $\frac{x^2}{\frac{9}{4}} + \frac{y^2}{\frac{5}{4}} = 1$. Es la elipse de semidiámetros $a = \frac{3}{2}$, $b = \frac{\sqrt{5}}{2}$.

ii ) Luego de elevar al cuadrado y operar algebraicamente se llega a $(x^2 + y^2)^2 - 2c^2(x^2 - y^2) = 0$ y en coordenadas polares resulta $\rho^2 - 2c^2 \cos 2\varphi = 0$. Es la lemniscata de Bernouilli.

*11-46.* Tener en cuenta que $\cos kx = \dfrac{e^{ikx} + e^{-ikx}}{2}$.

Efectuar $2 \sum\limits_{k=1}^{n} \cos kx = \sum\limits_{k=1}^{n} e^{ikx} + \sum\limits_{k=1}^{n} e^{-ikx}$ mediante las sumas de los $n$ primeros términos de las dos sucesiones geométricas. Luego de operar se llega a $1 + 2\sum\limits_{k=1}^{n} \cos kx = \dfrac{e^{i(n+1)x} - e^{-inx}}{e^{ix} - 1}$

*11-47.* No es una identidad. Basta dar un contraejerplo: $z = 2, w = 8$.

*11-48.* $z = -\sqrt{5} + \sqrt{2}\,i \Rightarrow \overline{z} = -\sqrt{5} - \sqrt{2}\,i \Rightarrow \rho = \sqrt{7}, \varphi = \text{arc tg } \dfrac{\sqrt{2}}{\sqrt{5}}$ en el tercer cuadrante. Se aplica la fórmula $\ln \overline{z} = \ln \sqrt{7} + i(\varphi + 2k\pi)$

*11-49.* i ) $e^z = e^w \Rightarrow e^x e^{iy} = e^u e^{iv} \Rightarrow x = u \ \wedge \ y = v + 2n\pi \Rightarrow z = x + yi =$
$= u + (v + 2n\pi)i = u + iv + 2n\pi i = w + 2n\pi i \Rightarrow z - w = 2n\pi i$ con $n \in Z$.

ii ) $z - w = 2n\pi i \Rightarrow z = w + 2n\pi i \Rightarrow e^z = e^{w+2n\pi i} \Rightarrow e^z = e^w . 1 \Rightarrow$
$\Rightarrow e^z = e^w$

*11-50.* i ) $2\cos z = e^{iz} + e^{-iz} = e^{i(x+iy)} + e^{-i(x+yi)} =$
$= e^{-y}(\cos x + i \operatorname{sen} x) + e^y(\cos x - i \operatorname{sen} x) =$
$= \cos x\,(e^y + e^{-y}) - i \operatorname{sen} x\,(e^y - e^{-y}) =$
$= 2\cos x \operatorname{ch} y - 2i \operatorname{sen} x \operatorname{sh} y \Rightarrow \cos z = \cos x \operatorname{ch} y - i \operatorname{sen} x \operatorname{sh} y$.

ii ) Utilizar el mismo procedimiento para sen $z$.

*11-51.* i) $z-\overline{z}=i \Rightarrow y=\frac{1}{2}$. Resulta $\left\{(x,y) \,/\, y=\frac{1}{2}\right\}$

ii) $|z|^2=z+\overline{z} \Rightarrow x^2+y^2=2x \Rightarrow x^2-2x+y^2=0 \Rightarrow x^2-2x+1+$ $+y^2=1 \Rightarrow (x-1)^2+y^2=1$. Es la circunferencia de centro $(1,0)$ y radio 1.

iii) $\overline{z}-z^{-1}=0 \Rightarrow z\overline{z}-1=0 \Rightarrow |z|^2=1 \Rightarrow x^2+y^2=1$. Es la circunferencia centrada en el origen, de radio 1.

iv) $z^{-1}+z=0 \Rightarrow z^2+1 \Rightarrow 0 \Rightarrow x^2-y^2+1+2xyi=0 \Rightarrow$
$\Rightarrow x^2-y^2+1=0 \;\wedge\; 2xy=0 \Rightarrow$
$\Rightarrow y^2-x^2=1 \;\wedge\; (x=0 \;\vee\; y=0) \Rightarrow$
$\Rightarrow (y^2-x^2=1 \;\wedge\; x=0) \;\vee\; (y^2-x^2=1 \;\wedge\; y=0, \Rightarrow$
$\Rightarrow (y=\pm 1 \;\wedge\; x=0) \;\vee\; (-x^2=1 \;\wedge\; y=0) \Rightarrow z=\pm i$

v) $z^{-1}+z\in \mathbf{R} \Rightarrow (x\neq 0 \;\wedge\; y=0) \;\vee\; x^2+y^2=1.$
Es la unión de la circunferencia de radio 1 con centro en el origen, y el eje real, salvo el origen.

vi) $z=\overline{z}^2 \Rightarrow x+yi=(x-yi)^2 \Rightarrow x+yi=x^2-y^2-2xyi \Rightarrow$
$\Rightarrow (x^2-y^2-x)+(-2xy-y)\,i=0 \Rightarrow$
$\Rightarrow x^2-x-y^2=0 \;\wedge\; y\,(2x+1)=0$

vii) $|z+i|=|z+2i| \Rightarrow |x+(y+1)i|=|x+(y+2)i| \Rightarrow$
$\Rightarrow x^2+(y+1)^2=x^2+(y+2)^2 \Rightarrow y^2+2y+1=y^2+4y+4 \Rightarrow$
$\Rightarrow 2y+3=0 \Rightarrow y=\frac{-3}{2}$. Resulta $\left\{(x,y) \,/\, y=-\frac{3}{2}\right\}$

*11-52.* a) $\sum_{k=0}^{100} i^k=1+i+i^2+\ldots+i^{100}=\frac{i^{101}-1}{i-1}=\frac{i-1}{i-1}=1$

b) $\prod_{k=1}^{100} i^k=i^{\sum_{k=1}^{100} k}=i^{\frac{100}{2}\cdot 101}=i^{5050}=i^2=-1$

*11-53.* Sabiendo que $|z_1+z_2|=|z_1|+|z_2|$ hay que probar que existe $\alpha\geq 0$ en $\mathbf{R}$, tal que $z_1=\alpha z_2$. Si alguno es 0, la propiedad se cumple obviamente. Supongamos entonces $z_1\neq 0$ y $z_2\neq 0$.

$|z_1+z_2|^2=|z_1|^2+|z_2|^2+2|z_1z_2| \Rightarrow (z_1+z_2)(\overline{z_1}+\overline{z_2})=$
$=|z_1|^2+|z_2|^2+2|z_1z_2| \Rightarrow 2\,\mathrm{Re}(z_1\overline{z_2})=2|z_1z_2|=2|z_1\overline{z_2}| \Rightarrow$
$\Rightarrow \mathrm{Re}(z_1\overline{z_2})=|z_1\overline{z_2}|$ (1)
Sean $z_1=x+yi \;\wedge\; z_2=u+iv \Rightarrow z_1\overline{z_2}=(xu+yv)+i\,(yu-xv)$ y por (1), se tiene:
$(xu+yv)^2=(xu+yv)^2+(yu-xv)^2 \Rightarrow yu-xv=0 \Rightarrow yu=xv$. De los casos posibles consideramos $v\neq 0 \Rightarrow x=\frac{u}{v} \Rightarrow z_1=x+yi=\frac{u}{v}\,y+yi=$

$=\frac{y}{v}\,(u+iv)=\alpha z_2$

Ahora bien, como $\operatorname{Re}(z_1\,\overline{z_2}) = |z_1|\,|z_2| \Rightarrow \operatorname{Re}(\alpha z_2 \overline{z_2}) = |\alpha z_2|\,|z_2| \Rightarrow$
$\Rightarrow \alpha |z_2|^2 = |\alpha|\,|z_2|^2 \Rightarrow |\alpha| = \alpha \Rightarrow \alpha \in \mathbf{R}^+ \cup \{0\}$.

*11-54.* i) $z = \dfrac{1}{-\sqrt{3}+i} = -\dfrac{\sqrt{3}}{4} - \dfrac{1}{4}\,i \Rightarrow \rho = \dfrac{1}{2} \;\wedge\; \varphi = 210^\circ$

$\Rightarrow z^4 = \left(\dfrac{1}{2}\right)^4 (\cos 840^\circ + i \operatorname{sen} 840^\circ) = \dfrac{1}{16}\,(\cos 120^\circ + i \operatorname{sen} 120^\circ) =$

$= \dfrac{1}{16}\,(-\cos 60^\circ + i \operatorname{sen} 60^\circ) = \dfrac{1}{16}\left(-\dfrac{1}{2} + i\,\dfrac{\sqrt{3}}{2}\right) = \dfrac{-1}{32} + i\,\dfrac{\sqrt{3}}{32}$

ii) $z = \dfrac{a}{\operatorname{sen}\alpha - i \operatorname{sen}\alpha} = \dfrac{a}{\operatorname{sen}\alpha}\,\dfrac{1}{1-i} = \dfrac{a}{\operatorname{sen}\alpha}\,\dfrac{1+i}{\sqrt{2}}$

Para $1+i$ es $\rho = \sqrt{2}$, $\varphi = 45^\circ$. Luego

$z^4 = \dfrac{a^4}{\operatorname{sen}^4 \alpha}\,(\cos 180^\circ - i \operatorname{sen} 180^\circ) = \dfrac{-a^4}{\operatorname{sen}^4}$

iii) $z = \dfrac{1+i}{\sqrt{3}-i}$

Para $1+i$ es $\rho = \sqrt{2}$ y $\varphi = 45^\circ$; para $\sqrt{3}-i$ es $\rho = 2$ y $\varphi = 330^\circ$.

$z = \dfrac{\sqrt{2}\,(\cos 45^\circ + i \operatorname{sen} 45^\circ)}{2\,(\cos 330^\circ + i \operatorname{sen} 330^\circ)} \Rightarrow z^4 = \dfrac{4\,(\cos 90^\circ + i \operatorname{sen} 90^\circ)}{16\,(\cos 1320^\circ + i \operatorname{sen} 1320^\circ)} =$

$= \dfrac{1}{4}\;\dfrac{i}{\cos 240^\circ + i \operatorname{sen} 240^\circ} = \dfrac{1}{4}\;\dfrac{i}{-\cos 60^\circ - i \operatorname{sen} 60^\circ} =$

$= \dfrac{1}{4}\;\dfrac{i}{-\dfrac{1}{2} - i\,\dfrac{\sqrt{3}}{2}} = \dfrac{i}{-2-2i\sqrt{3}} = -\dfrac{\sqrt{3}}{2} - \dfrac{1}{2}\,i$

*11-55.* i) $z\,\overline{w} + \overline{z}\,w = z\,\overline{w} + \overline{z\,\overline{w}} = 2\,Re\,(z\,\overline{w}) \Rightarrow Re\,(z\overline{w} + \overline{z}\,w) = z\,\overline{w} + \overline{z}\,w$.

ii) $z\,\overline{w} - \overline{z}\,w = z\,\overline{w} - \overline{z\,\overline{w}} = 2\,i\,Im\,(z\,\overline{w}) \Rightarrow Im\,(z\,\overline{w} - \overline{z}\,w) = \dfrac{1}{i}\,(z\,\overline{w} - \overline{z}\,w)$

*11-56.* Si $w$ es raíz cúbica primitiva de 1, entonces $w^2$ también lo es pues mcd $(2\,,3) = 1$. Teniendo en cuenta que $1 + w + w^2 = 0$ (ver 11-57), resulta

$(1-w)(1-w^2) = 1 - w^2 - w + w^3 = 1 - (w^2 + w) + 1 = 2 - (-1) = 3$

*11-57.* Para $n > 1$, si $w$ es raíz $n$-sima primitiva de 1, es $1 - w \neq 0$, y como
$(1 + w + w^2 + \ldots + w^{n-1})(1-w) = 1 - w^n = 0$
resulta $1 + w + w^2 + \ldots + w^{n-1} = 0$

*11-58.* $\left(-\dfrac{1}{2} + i\,\dfrac{\sqrt{3}}{2}\right)^n + \left(-\dfrac{1}{2} - i\,\dfrac{\sqrt{3}}{2}\right)^n =$

$= \left[\left(-\dfrac{1}{2} + i\,\dfrac{\sqrt{3}}{2}\right)^3\right]^k + \left[\left(-\dfrac{1}{2} - i\,\dfrac{\sqrt{3}}{2}\right)^3\right]^k = 1^k + 1^k = 2.$

## TRABAJO PRACTICO XII

*12-20.* i ) $a=2$ , $b=3$ , $c=4$
ii ) $a=1$ , $b=-1$ , $c=-1$

*12-21.* i ) $\overline{2}\,P - Q = \overline{4}\,X^4 + \overline{2}\,X^3 + \overline{3}\,X + \overline{5}$
ii ) $P\,.\,Q = \overline{1}\,X^5 + \overline{1}\,X^4 + \overline{3}\,X^3 + \overline{5}\,X^2 + \overline{1}\,X + \overline{3}$
iii) $P^2 - Q = \overline{4}\,X^8 + \overline{4}\,X^7 + X^6 + \overline{4}\,X^5 + \overline{2}\,X^4 + \overline{5}\,X + \overline{4}$
iv) $g\,(XP + 2\,Q) = 5$

*12-22.* $6 + 6\,.\,7 + 6\,.\,7^2 + 6\,.\,7^3$

*12-23.* No existen ya que en $\mathbf{R}\,[X]$ si A es de grado positivo, entonces de $A^2 = A$ se deduce $gA + gA' = gA \Rightarrow gA = 0$, lo que es imposible.

*12-24.* i ) $C=-2$ ; $R=-2$
ii ) $C=-1$ ; $R=-X^2-2\,X+3$
iii) $C=\mathbf{0}$ ; $R=2\,X^2-1$

*12-25.* Imponiendo al resto $(m^2 + 2\,m + 1)\,X$ la condición de ser el polinomio nulo, resulta $m = -1$.

*12-26.* i ) $C = -a\,X^2 - a^2\,X$ ; $R = -1$
ii ) Tener en cuenta que el opuesto de $\overline{2}$ es $\overline{3}$. Se obtienen
$C = \overline{3}\,X^3 + \overline{4}\,X^2 + \overline{3}\,X + \overline{3}$ ; $R = \overline{1}$
iii) $C = i\,X^3 + X^2 + (-2-i)\,X + (-1+2i)$ ; $R = 2 + 2i$
iv) Después de dividir el dividendo y divisor por tres se obtienen
$C = X^2 - 3\,X + 7$ y $\dfrac{R}{3} = \dfrac{64}{3}$ , o sea $R = 64$.

*12-27.* Aplicando 12.6.2 se obtienen:
i ) $X+1$ ii ) $X^2+4$ iii) $X^{11}-1$

*12-28.* Especializando X por $a$, se obtiene
$R = P(a)\,Q(a) - P(a)\,Q(a) = 0$, es decir $X - a \mid P\,.\,Q(a) - P(a)\,.\,Q$

*12-29.* En los tres anillos de polinomios se obtiene $P = (X+2)\,(X-2)\,(X+4)$.

*12-30.* Puede aplicarse 12.11.1, o bien por cómputo directo las raíces son $\pm\sqrt{2}$, $\pm\sqrt{3}$.

*12-31.* Las raíces de $P = X^4 - 10 X^2 + 1$ son
$\pm\sqrt{5 \pm 2\sqrt{6}} = \pm\sqrt{(\sqrt{2} \pm \sqrt{3})^2} = \pm(\sqrt{2} \pm \sqrt{3})$

*12-32.* De acuerdo con 12.9.2., si $\alpha$ es raíz doble de P, es raíz de $P' = 3x^2 + 4x - 4$. De P' son raíces $-2$ y $\frac{-2}{3}$. La primera es raíz doble de P y resulta $P = (x + 2)^2 (x - 2)$.

*12-33.* Basta efectuar $P = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4) = X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0$, donde
$a_3 = -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)$
$a_2 = \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \ldots + \alpha_3 \alpha_4$
$a_1 = -(\alpha_1 \alpha_2 \alpha_3 + \ldots + \alpha_2 \alpha_3 \alpha_4)$
$a_0 = \alpha_1 \alpha_2 \alpha_3 \alpha_4$. Ver 12.12.

*12-34.* $P = X^4 - 5X^2 + 4$

*12-35.* i ) A es irreductible en **Q** [X] pero no en **R** [X] pues $A = (X - \sqrt[3]{3})(X^2 + \sqrt[3]{3}X + \sqrt[3]{9})$

ii ) B es irreducible en ambos anillos pues $b^2 - 4ac < 0$.

iii) $C = (X+1)(X-1)(X^2+X+1)(X^2-X+1)$ es reducible en **Q** [X] y en **R** [X].

*12-36.* Si $a_2 = 0$, es trivial. Considerando $a_2 \neq 0$, se tiene $P = a_2 \left[\left(X + \frac{a_1}{2a_2}\right)^2 - \frac{\Delta}{4a_2^2}\right]$. Si $\Delta \geq 0$, entonces P es reducible. Luego P irreducible implica $\Delta < 0$.
Recíprocamente si $\Delta < 0$, entonces P es irreducible en **R** [X].

*12-37.* $P = X^2 + 2X - 4 \in \mathbf{Q}[X]$ con $\Delta = 4 + 16 = 20 > 0$, y es irreducible.

*12-38.* $P = \overline{3}X^2 + \overline{4}X + \overline{1}$

*12-39.* i ) Reflexividad: $B|0 \Rightarrow B|A - A \Rightarrow A \sim A$
Simetría: $A \sim A' \Rightarrow B|A - A' \Rightarrow B|A' - A \Rightarrow A' \sim A$
Transitividad: $A \sim A' \wedge A' \sim A'' \Rightarrow B|A - A' \wedge B|A' - A'' \Rightarrow$
$\Rightarrow B|A' - A'' \Rightarrow A' \sim A''$.

ii ) $K_A = \{P \in K[X] / P \sim A\}$ y como $P \sim A \Rightarrow B|P - A \Rightarrow P - A = CB \Rightarrow$
$\Rightarrow P = A + CB$. Luego $K_A = \{A + CB / C \in K[X]\}$

*12-40.* Probar, como en 5-12 y 5-13

i ) $A \sim A' \wedge C \sim C' \Rightarrow A + C \sim A' + C'$

ii ) $A \sim A' \wedge C \sim C' \Rightarrow AC \sim A'C'$

*12-41.* Demostrarlo en las siguientes etapas

i ) I es un subanillo de $K[X]$

ii) $Q \in I \ \wedge \ P \in K[X] \Rightarrow QP \in I$

I se llama ideal generado por A y B.

*12-42.* Sea $\{I_i\}$ con $i \in U$ una familia de ideales de $K[X]$. Con el criterio utilizado en 9-16 se prueba que $\bigcap_{i \in U} I_i$ es un subanillo de $K[X]$. Falta demostrar, de acuerdo con 12.5

$$A \in \bigcap_{i \in U} I_i \ \wedge \ P \in K[X] \Rightarrow AP \in \bigcap_{i \in U} I_i$$

lo que es inmediato.

*12-43.* Sean $I = \{S A_1 + T A_2 / S \ \wedge \ T \in K[X]\}$, y $\bigcap I_i$ la intersección de todos los ideales que contienen a $A_1$ y $A_2$. $A_1 = 1A_1 + 0A_2 \ \wedge \ A_2 = 0A_1 + 1A_2 \Rightarrow A_1 \in I \ \wedge \ A_2 \in I$, o sea I es un ideal que contiene a $A_2$ y a $A_2$. En consecuencia $\bigcap I_i \subset I$. Falta probar que $I \subset \bigcap I_i$ y para ello es suficiente demostrar: $P \in I \Rightarrow P \in \bigcap I_i$.

*12-44.* i ) $x = -2\sqrt[4]{i}$. Las cuatro raíces cuartas de $i$ se obtienen mediante

$$w_k = \sqrt[4]{\rho}\ \cos\left(\frac{\varphi + 2k\pi}{4} + i \operatorname{sen} \frac{\varphi + 2k\pi}{4}\right)$$

donde $\rho = 1$, $\varphi = \frac{\pi}{2}$ y $k = 0, 1, 2, 3$.

ii) $X^3 + X^2 + X + 1 = X^2(X+1) + (X+1) = (X+1)(X^2+1) = 0$

Resulta $x_1 = -1$, $x_2 = i$, $x_3 = -i$

iii) $iX^3 + 1 = 0 \Rightarrow X^3 = -\frac{1}{i} = -i \Rightarrow x = \sqrt[3]{-i}$. En este caso $\rho = 1$ y $\varphi = 3\frac{\pi}{2}$. Se aplica la fórmula de la parte i ) para $k = 0, 1, 2$.

*12-45.* i ) $x_1 + x_2 = 0 \Rightarrow -\dfrac{7(m-1)}{8m} = 0 \Rightarrow m = 1$

ii) $x_1 x_2 = 1 \Rightarrow \dfrac{1}{8m} = 1 \Rightarrow m = \dfrac{1}{8}$

iii) $\Delta = b^2 - 4ac = 0 \Rightarrow 49(m-1)^2 - 32m = 0$

se resuelve esta ecuación en $m$.

*12-46.* i ) Como $\alpha_3 = \alpha_1 + \alpha_2$ y $\alpha_1 + \alpha_2 + \alpha_3 = -2$ se tiene $\alpha_3 = -1$. Por otra parte, de $\alpha_1 + \alpha_2 = -1$ y $\alpha_2 \alpha_2 = 2$, se deduce que $\alpha_1$ y $\alpha_2$ son las raíces de la ecuación $t^2 + t + 2 = 0$ y resulta

$$\alpha_1 = -\frac{1}{2} + \frac{1}{2} i\sqrt{7} \quad , \quad \alpha_2 = -\frac{1}{2} - \frac{1}{2} i\sqrt{7}.$$

ii) De $\alpha_1\ \alpha_2\ \alpha_3 = 1$ y $\alpha_1\ \alpha_2 = -1$ se obtiene $\alpha_3 = -1$. Entonces P es divisible por $X + 1$. La aplicación de la regla de Ruffini determina el cociente $C = 2X^2 - 3X - 2$, cuyas raíces son $\alpha_1 = 2$ y $\alpha_2 = -\frac{1}{2}$

*12-47.* i ) Operando convenientemente se obtiene

$$- bx(b+x) \Rightarrow a(a+b+x)(x+b) \Rightarrow$$
$$\Rightarrow (a^2 \pm ab + ax)(x+b) + bx(b+x) = 0 \Rightarrow$$
$$\Rightarrow (x+b)(a^2 + ab + ax + bx) = 0 \Rightarrow$$
$$\Rightarrow x + b = 0 \ \vee \ (a+b)x + a(a+b) = 0 \Rightarrow x = -b \ \vee \ x = -a$$

si $a + b \neq 0$.

ii) Haciendo $x^4 = y$, se resuelve $y^2 + 2y + 1 = 0$ y se obtiene $y_1 = y_2 = -1$. Luego $x = \sqrt[4]{-1}$, siendo $\rho = 1$ y $\varphi = \pi$.

*12-48.* Considerando la condición $\alpha_1 = 2\alpha_2$ y las relaciones entre coeficientes y raíces, se obtiene $m = \pm 6$.

*12-49.* Como $(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^2 = \sum_{i=1}^{4} \alpha_i^2 + 2 \sum_{i<j}^{4} \alpha_i \alpha_j$, se tiene $(-3)^2 = \sum_{i=1}^{4} \alpha_i^2 + 2 \cdot \frac{5}{2} \Rightarrow \sum_{i=1}^{4} \alpha_i^2 = 4$.

*12-50.* El cambio de variable $x = y - 3$ conduce a $(y-3)^3 - 3(y-3)^2 + 2(y-3) = y^3 - 12y^2 + 45y - 60$.

# INDICE

Adición en C, 344
en N, 213
en Q, 297
en R, 319
en Z, 283
Algebra de Boole, 63, 210
Algoritmo de Euclides, 288
Amplitud de intervalos, 309
Anillo, 264
con identidad, 265
conmutativo, 265
de clases residuales, 267
de división, 265
de polinomios, 378, 383
ordenado, 276
propiedades, 266
sin divisores de cero, 267
Antisimetría, 75
Aplicación o función, 103
canónica, 116
A-reflexividad, 72
Argumento principal, 357
A-simetría, 74
A-transitividad, 74
Automorfismo, 153
En C, 350
Axiomas, 208,
de Peano, 212

Bicondicional, 6
Binomio de Newton, 179
Buena ordenación, 97, 167

Cambio de base, 334
Circuitos lógicos, 18
Clases de equivalencia, 79
residuales, 82, 157
Coclases, 255
Codominio, 102
Coeficiente principal, 382
Combinaciones con repetición, 199
simples, 198
Combinación lineal, 273
Combinatoria con repetición, 199, 200
simple, 197, 198
Compatibilidad, 154, 247, 319
Complejos conjugados, 349
Complejo imaginario, 343
real, 343, 350
Complementación, 36
Completitud de R, 326
Composición de funciones, 117
de relaciones, 68
Condición necesaria y suficiente, 7
Conectivos lógicos, 2
Congruencias en Z, 80
Conjunción, 3
Conjunto, 25
acotado, 94, 328
bien ordenado, 97
cociente, 79. 80
coordinables, 162
complementario, 36
de índices, 57
de partes, 34

diferencia de, 48
diferencia simétrica de, 50
equipotentes, 162
finito, 164
igualdad, 32
infinito, 165
inclusión, 30
intersección de, 38
numerable, 165, 301
operaciones generalizadas, 56
partición de, 84
producto cartesiano de, 53
unitario, 27
universal, 26
vacío, 26, 34
Cortaduras, 321
Cuerpo, 278
completo, 321
de los complejos, 341
de los racionales, 293
de los reales, 320
ordenado, 321
propiedades, 279

Densidad de **Q**, 299
de **Q** en **R**, 326
Descomposición factorial en **Z**, 292
de polinomios, 406
Diagramas de Hasse, 95
de Venn, 30
Diferencia de conjuntos, 48
simétrica, 7, 50
Distributividad, 150
División de polinomios, 384
entera, 287
Disyunción, 3
Doble implicación, 6
Dominio de relaciones, 66
de funciones, 102
de integridad, 272, 280
Dualidad, 211

Ecuaciones en un cuerpo, 279
en un grupo, 229
Elementos de un conjunto ordenado, 93
consecutivos, 95
coprimos, 275
inversos, 145, 221
maximales, 94
minimales, 94
neutro, 145, 220
primos, 276
regulares, 146
Encaje de intervalos, 309
Endomorfismo, 153
Epimorfismo, 153
Especialización, 396
Estructura algebraica, 219
de anillo, 264
de cuerpo, 278
de grupo, 225
de monoide, 220
de semigrupo, 220
Extremo superior, 94, 328
inferior, 94
Exponencial compleja, 366, 369

Factoriales, 176
Factirización en un anillo, 274
en **Z**, 292
de polinomios, 389
Forma binómica, 347
exponencial, 366
polar, 356
Fórmula de De Moivre, 359
de Taylor, 409
Función, 102
biyectiva, 111
canónica, 116
característica, 140
clasificación de 110, 111
compuesta, 117
constante, 114
creciente, 191
de probabilidad, 140
entre intervalos, 186
estrictamente creciente, 189, 194

extensión de, 137
identidad, 115
inversa, 121, 127
inyectiva, 110
factorial, 176
mantisa, 138
parte entera, 138
proposicional, 14
proyección, 115
representación de, 105
restricción de, 137
signo, 109
sucesor, 213
valor absoluto, 125, 285

Grado de polinomios, 379
Grupo, 225
abeliano, 226
aditivo, 229
cíclico, 257
cociente, 251, 254
de automorfismos, 262
de raíces cúbicas, 243
de raíces de la unidad, 371
de transformaciones, 228
finito, 259
generadores de, 257
morfismo de, 237, 239
multiplicativo, 229
propiedades, 228

Homomorfismos, 151
de grupos, 237

Ideal, 272, 388
Idempotencia, 9
Imagen, 66, 128, 242
inversa, 131
Implicación, 4
Implicaciones asociadas, 11
Inclusión, 30, 33, 34
Indeterminada, 381
Indice de un grupo, 260
Inducción completa, 167
Infimo, 94
Intersección, 38
Intervalos, 164, 309
Inverso, 230
Involución, 9
Isomorfismo, 153, 284, 298, 321, 347

Ley cancelativa, 269
de composición interna, 142, 144
de composición externa, 158
de De Morgan, 10, 46, 47
distributiva, 9, 46, 150
inducida, 155, 283, 297
lógica, 8
Logaritmación en **C**, 333
en **R**, 367

Matrices, 149, 153, 270
simétricas, 234
Máximo común divisor, 274, 288, 389
Método de Horner, 411
Módulo en **C**, 351
propiedades del, 351
Monoide, 220
Monomorfismo, 153
Morfismo, 151
de grupos, 237
Multiplicación en **C**, 344
en **Q**, 297
en **N**, 213
en **R**, 320, 325
en **Z**, 283

Negación de implicaciones, 12
de proposiciones, 2, 16
No reflexividad, 72
No simetría, 73
No transitividad, 74
Núcleo, 240
Numerabilidad de **Q**, 301
de **Z**, 164
Número cardinal, 163

combinatorio, 177
complejo, 341
entero, 281
irracional, 315
primo, 290
racional, 295
real, 308, 315, 323

Orden amplio, 90
de un grupo, 259
estricto, 92
parcial, 91
total, 91
Operaciones con subgrupos, 235
en forma exponencial, 367
en forma polar, 358

Par ordenado, 53
Partición, 84, 87
Permutaciones simples, 198
con repetición, 199
Polinomio, 378
adición de, 380
coprimos, 392
derivado, 400
división de, 384
grado de, 379, 383
multiplicación de, 380
nulo, 378
primo, 393
raíz de, 397
Potencia de un binomio, 179
Potencia de R, 335
Potenciación en C, 335
en R, 359
Preimágenes, 131
Primer elemento, 93
Principio de buena ordenación, 167
de inducción completa, 168
Producto cartesiano, 53
Proposición, 1.

Radicación en C, 329
en R, 354, 362
Raíces de polinomios, 397, 403, 405,
múltiples, 399
Razonamiento deductivo, 13
Reflexividad, 71
Regla de Horner, 411
de Ruffini, 387
Regularidad, 146
Relación binaria, 64
circular, 99
composición de, 68
de equivalencia, 77, 88, 313
de orden, 90, 218, 299, 324
dominio de, 66,
en un conjunto, 69
funcional, 102
imagen de, 67
inversa, 67
propiedades, 71
representación de, 65
Relaciones entre coeficientes y raíces, 407
Restricción, 137

Semigrupo, 220
Silogismo hipotético, 13
Sistemas axiomáticos, 208
Sistema de Peano, 213
Subgrupos, 231
de matrices, 234
distinguidos, 248
intersección de, 235
normales o invariantes, 252
unión de, 236
Sucesión, 165
monótona contigua, 312
Subanillos, 272
Sumatorias, 170
Supremo, 94

Traslaciones de un grupo, 258
Términos primitivos, 208
Teorema de compatibilidad, 155, 247

de descomposición factorial, 292, 394
de Euclides, 292
de Gauss, 403
de inducción completa, 167
de Lagrange, 260
de las relaciones de equivalencia, 85
del resto, 397
fundamental del álgebra, 406

Ultimo elemento, 94
Unidad imaginaria, 347
Unión de conjuntos, 42
disjunta, 58

Valor absoluto, 285
Variaciones con repetición, 199
simples, 197

Este libro se terminó de imprimir
el 16 de marzo de 1981 en los
Talleres Gráficos LITODAR
Brasil 3215 - Buenos Aires

Tirada de la edición: 5 000 ejemplares.

EDITORIAL
"EL ATENEO"
BUENOS AIRES